

PROTECTION OF ASSETS

PHYSICAL SECURITY



PROTECTION OF ASSETS

PHYSICAL SECURITY

PROTECTION OF ASSETS

PHYSICAL SECURITY



Copyright © 2012 by ASIS International

ISBN 978-1-934904-37-4

Protection of Assets is furnished with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. It is designed as a ready reference and guide to the covered subjects. While every effort has been made to ensure accuracy of contents herein, it is not an official publication and the publisher can assume no responsibility for errors or omissions.

All rights reserved. No part of this publication may be reproduced, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written consent of the copyright owner.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

ACKNOWLEDGMENTS

ASIS International (ASIS), the world's leading society for security professionals, originally founded in 1955 as the American Society for Industrial Security, acquired *Protection of Assets* in December 2003. The acquisition of this work underscores the Society's leadership role in professional education. It is the sincere desire of ASIS and its editorial staff to continue to enhance the value of this important reference.

Protection of Assets, which has been in existence since 1974, is recognized as the premier reference for security professionals and the publisher wishes to acknowledge the two founding authors and subsequent editors.

Timothy J. Walsh, CPP

Richard J. Healy, CPP

Timothy L. Williams, CPP
Managing Editor

Editorial Associates

David G. Aggleton, CPP
Milton E. Moritz, CPP

Mike Hodge, J.D.

Sanford Sherizon, Ph.D., CISSP

Timothy J. Walsh, CPP, Editor Emeritus

As we move forward, confronted with issues that present a challenge to the security industry, our mission is to ensure that *Protection of Assets* provides the strategic solutions necessary to help professionals meet the demands of the 21st century and beyond. We also pledge to assemble a group of subject matter experts who will enhance this reference as necessary to achieve our mission.

Michael E. Knoke, CPP
Managing Editor

Mary Lynn Garcia, CPP
Co-Editor

Eva Giercuskiewicz, MLS, Project Manager

Evangeline Pappas, Production Manager

Peter E. Ohlhausen, Technical Editor



PREFACE

OBJECTIVES OF PROTECTION OF ASSETS

Protection of Assets (POA) is intended for a security professional to find current, accurate, and practical treatment of the broad range of asset protection subjects, strategies, and solutions in a single source.

The need for such a comprehensive resource is quite widespread according to the editors, writers, and many professional colleagues whose advice has been sought in compiling this text. The growing size and frequency of all forms of asset losses, coupled with the related increasing cost and complexity of countermeasures selection, demand a systematic and unified presentation of protection doctrine in all relevant areas, as well as standards and specifications as they are issued. Of course, it would be presumptuous to assume that any small group of authors could present such material unaided. It is, therefore, a fundamental objective of *Protection of Assets* to draw upon as large a qualified source base as can be developed. The writers, peer reviewers, and editors attempt to distill from the available data, common or recurrent characteristics, trends, and other factors, which identify or signal valid protection strategies. The objective is to provide a source document where information on any protection problem can be obtained.

READERSHIP

Protection of Assets is intended for a wide readership: all security professionals and business managers with asset protection responsibility. The coherent discussion and pertinent reference material in each subject area should help the reader conduct unique research that is effective and organized. Of particular significance are the various forms, matrices, and checklists that give the reader a practical start toward application of the security theory to his or her own situation. *POA* also serves as a central reference for students pursuing a program in security or asset protection.

DIALOGUE

We hope that *Protection of Assets* becomes an important source of professional insight for those who read it and that it stimulates serious dialogue between and among security professionals. Any reader who is grappling with an unusual, novel, or difficult security problem and would appreciate the opinions of others is encouraged to write a succinct statement describing the problem and send it to us at ASIS [protectionofassets@asisonline.org]. At the reader's request his identity will not be disclosed, but the problem will be published with invitations for comment. Readers are also encouraged to communicate agreement or disagreement with strategies or applications recommended in *POA* and to suggest alternatives. We reserve the right to publish or refrain from publishing submitted material. The editors also solicit statements of reader opinion on matters of asset protection policy in which a cross-sectional view would be helpful.

SUPPLEMENTAL TRAINING

Readers with supervisory or management responsibility for other security and asset protection personnel will find *POA* to be a useful resource from which to assign required readings. Such readings could be elements of a formal training syllabus and could be assigned as part of related course sessions.

With all these objectives in mind, we present to you *Protection of Assets*, in the sincere belief it will enhance your expertise in the security field.

Michael E. Knoke, CPP

Managing Editor

CONTRIBUTORS

The success of this publication is directly related to the peer review process recognized by most professions. Security professionals, members of academia, and other subject matter experts were involved in contributing current information, conducting research, reviewing submissions, and providing constructive comments so that we are able to provide a publication that is recognized as the “go to” reference for security professionals worldwide.

It is with sincere appreciation that I wish to thank the below-named individuals who contributed to *Protection of Assets*.

| | | |
|-----------------------------|--------------------------------|-------------------------------|
| Teresa M. Abrahamsohn, CPP | Lucien G. Canton, CPP | Donald J. Fergus |
| Sean A. Ahrens, CPP | James P. Carino, Jr., CPP | Eugene F. Ferraro, CPP, PCI |
| Marene N. Allison | Sue Carioti | James H. Fetzer, III, CPP |
| Randy I. Atlas, CPP | James S. Cawood, CPP, PCI, PSP | Michael T. Flachs, CPP |
| George J. Barletta, CPP | Steve Chambers, CPP, PSP | Linda F. Florence, Ph.D., CPP |
| Mark H. Beaudry, CPP | Richard E. Chase, CPP | Richard H. Frank, CPP |
| Regis W. Becker, CPP | John C. Cholewa, III, CPP | Kenneth M. Freeman, CPP |
| Brent Belcoff, CPP | Tom M. Conley, CPP | Peter J. French, CPP |
| Howard J. Belfor, CPP | Geoffrey T. Craighead, CPP | Mary Lynn Garcia, CPP |
| Adolfo M. Benages, CPP | Michael A. Crane, J.D., CPP | John W. Gehrlein, CPP |
| Lawrence K. Berenson, CPP | Bruce A. Dean, CPP | Eva Giercuskiewicz, MLS |
| Alexander E. Berlonghi | Fritz X. Delinski | Gregory A. Gilbert, CPP |
| Raymond J. Bernard, PSP | Edward P. De Lise, CPP | Frederick G. Giles, CPP |
| Henri A. Berube | David A. Dobbins, PSP | Timothy D. Giles, CPP, PSP |
| Martin T. Biegelman, J.D. | Colin Doniger, CPP, PSP | David H. Gilmore, CPP |
| Daniel E. Bierman, CPP, PSP | Clifford E. Dow, CPP | Christopher Giusti, CPP |
| Patrick C. Bishop, CPP | Christina M. Duffey, CPP | Leo Gonnering, PSP |
| Dennis R. Blass, CPP, PSP | Brandon Dunlap | Brian D. Gouin, PSP |
| Keith C. Blowe, CPP | Nick Economou | Richard P. Grassie, CPP |
| Paul F. Boyarin, CPP, PCI | Cheryl D. Elliott, CPP, PCI | Benjamin P. Greer |
| Tom Boyer | James W. Ellis, CPP, PSP | Steven R. Harris |
| Pete Brake, Jr., CPP | William R. Etheridge | Ronald D. Heil, CPP |
| Darryl R. Branham, CPP | Gregory Alan Ewing, CPP, PSP | Ed Heisler, CPP, PSP |
| Joseph P. Buckley, III | Kenneth G. Fauth, CPP | Richard J. Heffernan, CPP |
| Jason Caissie, CPP, PSP | Lawrence J. Fennelly | Chris A. Hertig, CPP |

| | | |
|-------------------------------|----------------------------------|----------------------------------|
| William T. Hill, CPP | Wayne Morris, CPP, PSP | Shari Shovlin |
| Ronald W. Hobbs, CPP | Patrick M. Murphy, CPP, PSP | Marc Siegel, Ph.D. |
| Mark D. Hucker, CPP | Carla Naude, CPP | Laurie Simmons, CPP, PSP |
| W. Geoffrey Hughes, PCI | James W. Nelson | Dennis Smith, CPP |
| John L. Hunepohl | Robert L. Oatman, CPP | Stan Stahl, Ph.D. |
| Gregory L. Hurd, CPP | Gerald A. O'Farrell, CPP | Paul J. Steiner, Jr., CPP |
| Gregory W. Jarpey, PSP | Peter E. Ohlhausen | Pamela M. Stewart, PCI |
| Sheila D. Johnson, CPP, PSP | Leonard Ong, CPP | Dan E. Taylor, Sr., CPP |
| Thomas R. Jost | Harm J. Oosten, CPP | Lynn A. Thackery, CPP, PSP |
| Diane Horn Kaloustian | S. Steven Oplinger | Mark L. Theisen, CPP |
| Cathy M. Kimble, CPP | Denis A. O'Sullivan, CPP | Dave N. Tyson, CPP |
| R. Michael Kirchner, CPP | Jaime P. Owens, CPP | Joann Ugolini, CPP, PSP |
| Glen W. Kitteringham, CPP | Gerard P. Panaro, J.D. | Darleen Urbanek |
| Michael E. Knoke, CPP | James F. Pastor, Ph.D. | Mike VanDrongelen, CPP, PCI, PSP |
| Terrence J. Korpai | David G. Patterson, CPP, PSP | Karim Vellani, CPP |
| James M. Kuehn, CPP | John T. Perkins, CPP | Barry J. Walker, CPP |
| David Lam, CPP | Karl S. Perman | Michael W. Wanik, CPP |
| Rich LaVelle, PSP | Kevin E. Peterson, CPP | Roger D. Warwick, CPP |
| Robert F. Leahy, CPP, PSP | Charlie R. A. Pierce | Fritz Weidner |
| Robert E. Lee | Doug Powell, CPP, PSP | Richard C. Werth, CPP |
| Jeff Leonard, CPP, PSP | Patrick K. Quinn, CPP | Allan R. Wick, CPP, PSP |
| Todd P. Letcher | Roy A. Rahn, CPP | Anthony S. Wilcox, CPP |
| Emblez Longoria, CPP, PSP | John D. Rankin, CPP | Donald S. Williams, CPP |
| Cynthia Long | William G. Rauen, CPP | Reginald J. Williams, CPP |
| Richard E. Maier, CPP | David L. Ray, LL.B. | Richard F. Williams, CPP |
| Loye A. Manning, CPP, PSP | Joseph Rector, CPP, PCI, PSP | Timothy L. Williams, CPP |
| Robert L. Martin, CPP | Ty L. Richmond, CPP | Gavin Wilson, PSP |
| Ron Martin, CPP | Lisa M. Ruth | Coleman L. Wolf, CPP |
| Roger B. Maslen, CPP | Jeffrey J. Ryder, Jr., CPP, PSP | Loftin Woodiel, CPP |
| Judith G. Matheny, CPP | Mark A. Sanna, CPP | Richard P. Wright, CPP |
| Edward F. McDonough, Jr., CPP | Stephen Saravara, III, J.D., CPP | Allison Wylde |
| Richard A. Michau, CPP | Charles A. Sennewald, CPP | Richard Y. Yamamoto, CPP |
| Bonnie S. Michelman, CPP | Dennis Shepp, CPP, PCI | Scott S. Young, CPP |
| Owen J. Monaghan, CPP | | |

TABLE OF CONTENTS

PREFACE

CONTRIBUTORS

INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS 1

PART I: PHYSICAL PROTECTION SYSTEM GOALS AND OBJECTIVES 3

Chapter 1. **PROBLEM DEFINITION** 5

| | | |
|-------|-----------------------------------------|----|
| 1.1 | Overview | 5 |
| 1.2 | Risk Assessment/Management | 6 |
| 1.3 | Threat Definition | 10 |
| 1.4 | Historical Experience | 13 |
| 1.5 | Asset Identification | 15 |
| 1.6 | Loss Impact | 15 |
| 1.7 | Vulnerability Assessment (VA) | 20 |
| 1.6.1 | VA Team | 20 |
| 1.6.2 | VA Concepts | 21 |
| 1.6.3 | VA Objectives | 22 |
| 1.6.4 | Risk Assessment | 25 |
| | References | 27 |

PART II: PHYSICAL PROTECTION SYSTEM DESIGN 29

Chapter 2. **DESIGN PRINCIPLES AND CONCEPTS** 31

| | | |
|-------|----------------------------------------------------|----|
| 2.1 | PPS Characteristics | 31 |
| 2.1.1 | Protection-in-Depth | 31 |
| 2.1.2 | Minimum Consequence of Component Failure | 32 |
| 2.1.3 | Balanced Protection | 32 |
| 2.2 | Design Criteria | 33 |
| 2.3 | Additional Design Elements | 34 |

PPS FUNCTION: **DETERRENCE** 36

Chapter 3. **CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN** 37

| | | |
|-------|--------------------------------------------------------|----|
| 3.1 | CPTED Theory | 37 |
| 3.1.1 | CPTED Fundamentals | 38 |
| 3.1.2 | History of CPTED | 42 |
| 3.1.3 | Crime Prevention Assumptions | 44 |
| 3.1.4 | Contemporary Thinking on Crime and Criminals | 45 |
| 3.2 | Reducing Crime Through Architectural Design | 55 |
| 3.2.1 | Building Planning and Design | 55 |
| 3.2.2 | Office Buildings | 61 |
| 3.2.3 | Industrial Buildings | 66 |
| 3.2.4 | Parking Facilities | 67 |

| | | |
|-------------------------------------------|------------------------------------|----|
| 3.2.5 | Schools | 72 |
| 3.2.6 | Automated Teller Machines. | 75 |
| 3.2.7 | U.S. Federal Buildings | 78 |
| Appendix A: CPTED Sample Survey | | 81 |
| References | | 87 |

| | | |
|------------------------------------------|--|-----------|
| PPS FUNCTION: DETECTION | | 90 |
| Chapter 4. SENSORS | | 91 |

| | | |
|----------------------|-----------------------------------------------|-----|
| 4.1 | Key Sensor Concepts | 91 |
| 4.1.1 | Performance Characteristics | 92 |
| 4.1.2 | Alarm Initiation Conditions. | 94 |
| 4.1.3 | Operating Conditions | 94 |
| 4.2 | Standards | 94 |
| 4.2.1 | UL Standards | 94 |
| 4.2.2 | ASTM Standards | 96 |
| 4.2.3 | Other Standards and Specifications | 96 |
| 4.3 | Exterior Sensors. | 97 |
| 4.3.1 | Classification | 97 |
| 4.3.2 | Types of Exterior Intrusion Sensors | 99 |
| 4.3.3 | Other Exterior Sensor Concepts | 105 |
| 4.4 | Interior Sensors | 114 |
| 4.4.1 | Classification | 115 |
| 4.4.2 | Types of Interior Intrusion Sensors | 116 |
| 4.4.3 | Other Interior Sensor Concepts | 127 |
| 4.5 | Summary. | 130 |
| References | | 132 |

| | | |
|-------------------------------------------------------------------|--|------------|
| Chapter 5. VIDEO SUBSYSTEMS AND ALARM ASSESSMENT | | 133 |
|-------------------------------------------------------------------|--|------------|

| | | |
|-------|-----------------------------------------------------------------|-----|
| 5.1 | Theory of Visual Security. | 134 |
| 5.2 | Uses of Video Subsystems in Security | 135 |
| 5.2.1 | Subject Identification | 136 |
| 5.2.2 | Action Identification. | 136 |
| 5.2.3 | Scene Identification | 137 |
| 5.3 | Analog System Components. | 137 |
| 5.4 | Digital System Components. | 139 |
| 5.5 | System Design. | 141 |
| 5.6 | Equipment Selection | 150 |
| 5.6.1 | Camera | 150 |
| 5.6.2 | Lenses | 151 |
| 5.7 | Camera Formats and Lenses | 154 |
| 5.8 | Controlling Software | 156 |
| 5.9 | Recording Systems | 158 |
| 5.10 | Additional Design Considerations for Video Assessment | 159 |

| | | |
|-------------------------------------------------------------|--------------------------------------------------------------|------------|
| 5.11 | Evaluation of Video Assessment Systems | 166 |
| 5.12 | Where CCTV Is Heading | 168 |
| Chapter 6. LIGHTING | | 169 |
| 6.1 | Lighting and Lighting Definitions. | 169 |
| 6.2 | Lighting Systems | 175 |
| 6.3 | Lighting Economics. | 176 |
| 6.4 | Starting and Restrike | 178 |
| 6.5 | Security Lighting Applications | 179 |
| 6.6 | Security Lighting and Closed-Circuit Video Systems | 182 |
| 6.7 | Standards for Security Lighting Levels | 183 |
| | References | 185 |
| Chapter 7. ALARM COMMUNICATION AND DISPLAY | | 187 |
| 7.1 | AC&D Attributes | 187 |
| 7.2 | Alarm Communication Subsystem | 189 |
| 7.3 | Security Communications | 190 |
| 7.3.1 | Wire and Cable Communications | 191 |
| 7.3.2 | Wireless Communications | 198 |
| 7.3.3 | Microwave Transmissions | 204 |
| 7.3.4 | Laser Communication. | 204 |
| 7.3.5 | Interconnection | 205 |
| 7.4 | Communications Security | 206 |
| 7.4.1 | Line Protection | 206 |
| 7.4.2 | Scramblers | 207 |
| 7.5 | Alarm Control and Display. | 210 |
| 7.5.1 | Ergonomics: Human Factors | 211 |
| 7.5.2 | Ergonomics: Graphical Displays | 213 |
| 7.6 | Summary. | 215 |
| Chapter 8. ENTRY CONTROL | | 217 |
| 8.1 | Personnel Entry Control | 218 |
| 8.1.1 | Personal Identification Number | 218 |
| 8.1.2 | Token | 219 |
| 8.1.3 | Photo Identification Badge | 219 |
| 8.1.4 | Coded Credential. | 220 |
| 8.1.5 | Personnel Identity Verification (Biometrics) | 223 |
| 8.1.6 | Personnel Entry Control Bypass | 228 |
| 8.2 | Contraband Detection | 228 |
| 8.2.1 | Manual Search | 228 |
| 8.2.2 | Metal Detectors. | 229 |
| 8.2.3 | Package Search | 231 |

| | | |
|--------------------------------------------|------------------------------------------------------|-----|
| 8.3 | Locks | 239 |
| 8.3.1 | Mechanical Locks | 240 |
| 8.3.2 | Electrified Locking Mechanisms | 244 |
| 8.3.3 | Designing Secure Locking Systems. | 248 |
| 8.4 | System Integration and Installation Issues | 251 |
| 8.4.1 | Procedures | 253 |
| 8.4.2 | Administration | 254 |
| 8.5 | Summary. | 255 |
| | References | 257 |
| PPS FUNCTION: DELAY | | 258 |
| Chapter 9. DELAY BARRIERS | | 259 |
| 9.1 | Barrier Types and Principles. | 259 |
| 9.2 | Perimeter Barriers | 262 |
| 9.2.1 | Fences | 263 |
| 9.2.2 | Gates. | 263 |
| 9.2.3 | Vehicle Barriers. | 264 |
| 9.3 | Structural Barriers | 265 |
| 9.3.1 | Walls | 266 |
| 9.3.2 | Doors | 267 |
| 9.3.3 | Windows and Utility Ports | 270 |
| 9.3.4 | Roofs and Floors | 272 |
| 9.3.5 | Dispensable Barriers. | 273 |
| 9.3.6 | Procedures | 275 |
| 9.4 | Safes | 276 |
| 9.4.1 | Record Safes for Fire Protection | 276 |
| 9.4.2 | Safes Designed to Protect Valuables | 279 |
| 9.5 | Vaults. | 281 |
| 9.5.1 | Fire-Resistive Vaults | 281 |
| 9.5.2 | Media Storage and Protection | 282 |
| 9.5.3 | Vaults for Protection Against Forced Entry | 283 |
| 9.6 | Summary. | 285 |
| | References | 287 |
| PPS FUNCTION: RESPONSE | | 288 |
| Chapter 10. RESPONSE | | 289 |
| 10.1 | Security Operations. | 289 |
| 10.2 | General Considerations | 290 |
| 10.3 | Contingency Planning | 291 |
| 10.4 | Performance Measures. | 294 |
| | References | 296 |
| Part II Summary | | 297 |

| | |
|---------------------------------------------------------------------|-----|
| PART III: ANALYSIS | 299 |
| Chapter 11. ANALYSIS OF THE PHYSICAL PROTECTION SYSTEM | 301 |
| 11.1 Introduction | 301 |
| 11.2 Analysis Overview | 302 |
| 11.3 Analysis Tools | 304 |
| 11.3.1 Qualitative Analysis—CARVER | 305 |
| 11.3.2 Performance-Based Analysis | 306 |
| 11.3.3 Analysis Process | 307 |
| 11.4 Calculate System Effectiveness | 314 |
| 11.4.1 Upgrade Analysis | 314 |
| 11.5 Summary | 315 |
| References | 316 |
| PART IV: IMPLEMENTATION | 317 |
| Chapter 12. IMPLEMENTATION OF THE PHYSICAL PROTECTION SYSTEM | 319 |
| 12.1 Introduction | 319 |
| 12.2 Systems Design Process | 320 |
| 12.3 Initial Phases | 322 |
| 12.3.1 Basis of Design | 325 |
| 12.3.2 Conceptual Design | 325 |
| 12.4 Design Criteria | 327 |
| 12.4.1 Codes and Standards | 327 |
| 12.4.2 Quality | 328 |
| 12.4.3 Capacity | 328 |
| 12.4.4 Performance | 329 |
| 12.4.5 Features | 329 |
| 12.4.6 Cost | 329 |
| 12.4.7 Operations | 330 |
| 12.4.8 Culture and Image | 330 |
| 12.4.9 Monitoring and Response | 330 |
| 12.4.10 Preliminary Cost Estimate | 331 |
| 12.5 Design Team | 333 |
| 12.6 Design and Documentation Phase | 335 |
| 12.6.1 Contractual Details | 336 |
| 12.6.2 Specifications | 336 |
| 12.6.3 Drawings | 338 |
| 12.6.4 Design Coordination | 345 |
| 12.7 Construction Document Review, Approvals, and Issue | 346 |
| 12.8 Procurement Phase | 347 |
| 12.8.1 Sole Source Procurement | 348 |
| 12.8.2 Request for Proposal (RFP) | 348 |

| | | |
|--------------|----------------------------------------------------|------------|
| 12.8.3 | Invitation for Bid (IFB) | 349 |
| 12.8.4 | Procurement Process | 349 |
| 12.9 | Installation and Operation. | 351 |
| 12.9.1 | Planning the Installation | 351 |
| 12.9.2 | Component Installation | 352 |
| 12.9.3 | Other Features and Considerations | 356 |
| 12.9.4 | Tuning the System | 360 |
| 12.9.5 | Maintaining the Operating Procedures | 361 |
| 12.10 | Training | 362 |
| 12.10.1 | General Training Requirements | 363 |
| 12.10.2 | Training Topics. | 363 |
| 12.11 | Testing and Warranty Issues. | 366 |
| 12.11.1 | Factory Acceptance Testing. | 367 |
| 12.11.2 | Site Acceptance Testing | 368 |
| 12.11.3 | Reliability or Availability Testing | 370 |
| 12.11.4 | After-Implementation Testing | 371 |
| 12.11.5 | Warranty Issues. | 372 |
| 12.12 | Maintenance, Evaluation, and Replacement | 373 |
| 12.12.1 | Remedial Maintenance | 374 |
| 12.12.2 | Preventive Maintenance. | 379 |
| 12.12.3 | Evaluation and Replacement | 381 |
| 12.13 | Summary. | 381 |
| | Appendix A: Estimation | 382 |
| | Appendix B: Specification. | 386 |
| | References | 392 |
| INDEX | | 395 |

TABLE OF FIGURES

| | | |
|-------|-------------------------------------------------------------------|-----|
| 1-1 | Sample Consequence Table. | 19 |
| 4-1 | Glass-Break Sensor. | 117 |
| 6-1 | Natural and Visual Light Levels. | 171 |
| 6-2 | Reflectance Measurements | 172 |
| 6-3 | Color Temperature. | 173 |
| 6-4 | Color Rendition Index | 174 |
| 6-5 | Lamp Efficacy, Life, and Cost | 177 |
| 6-6 | Lamp Starting and Restrike Times | 178 |
| 6-7 | Lighting and Security Perceptions | 181 |
| 6-8 | Guidelines for Minimum Lighting Levels | 184 |
| 7-1 | Multiplexing on a Pair of Wires | 195 |
| 7-2 | Elements of Multiplexing | 195 |
| 7-3 | Simplified Time Division Multiplex System. | 196 |
| 7-4 | Typical Arrangement for Frequency Division Multiplexing | 197 |
| 7-5 | Frequency Inverter. | 207 |
| 7-6 | Bandsplitter. | 208 |
| 7-7 | Placement of Operator Controls in an AC&D Console. | 212 |
| 9-1 | Underwriters Laboratories Label Designations. | 279 |
| 12-1 | Systems Design Process | 320 |
| 12-2 | Requirements Analysis | 324 |
| 12-3 | Countermeasures Development Table | 327 |
| 12-4 | Sample Cost Estimate Format | 333 |
| 12-5 | Typical Floor Plan | 339 |
| 12-6 | Typical Drawing Device Symbolology | 341 |
| 12-7 | Security Door Elevation | 342 |
| 12-8 | Sample Riser Diagram | 343 |
| 12-9 | Sample Door Schedule | 344 |
| 12-10 | Sample Camera Schedule | 344 |
| 12-11 | Sample Estimate | 385 |

INTRODUCTION TO PHYSICAL PROTECTION SYSTEMS

This book describes the design and evaluation of a physical protection system (PPS). A PPS is an important part of overall security for a site or enterprise.

ASIS International (2009, Facilities) defines physical security as

that part of security concerned with physical measures designed to safeguard people; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against a security incident.

Physical security uses people, procedures, and technology (both hardware and software) to protect assets. Hardware components of a PPS include sensors, cameras, lighting, alarm monitoring equipment, entry and exit control devices, barriers, and guard force equipment, such as radios, handcuffs, duress devices, and weapons. People, procedures, and technology are combined to provide the PPS functions. The primary functions of a PPS are detection, delay, and response; a secondary function is deterrence (Garcia, 2008, pp. 2-6).

Development of a security system starts with a definition of the problem to be solved and a determination of the system’s goals and objectives. The next major stages are design, analysis, and implementation. Within the design stage, specific security equipment and measures are divided into four groups, according to function (deterrence, detection, delay, and response).

This book organizes the development of a physical protection system as follows:

| | | |
|----------|----------------------|----------------------------------------------------------|
| Part I | Goals and Objectives | Chapter 1. Problem Definition |
| Part II | Design | Chapter 2. Design Principles and Concepts |
| | | Chapter 3. Crime Prevention Through Environmental Design |
| | | Chapter 4. Sensors |
| | | Chapter 5. Video Subsystems and Alarm Assessment |
| | | Chapter 6. Lighting |
| | | Chapter 7. Alarm Communication and Display |
| | | Chapter 8. Entry Control |
| | | Chapter 9. Delay Barriers |
| | | Chapter 10. Response |
| | | Part II. Summary |
| Part III | Analysis | Chapter 11. Analysis |
| Part IV | Implementation | Chapter 12. Implementation |

Physical protection systems raise many legal considerations. Readers are encouraged to consult the legal issues volume of *Protection of Assets*.

PART I

PHYSICAL PROTECTION SYSTEM GOALS AND OBJECTIVES

This part of the book addresses the importance of determining the physical protection system's goals and objectives. Its discussion is presented in Chapter 1, Problem Definition.

CHAPTER 1

PROBLEM DEFINITION

1.1 OVERVIEW

The implementation of a PPS is a complex and challenging task. The security manager at a site should lead the effort to create a PPS that meet the organization's goals and objectives. The security manager should engineer the PPS by using the building blocks of people, procedures, and technology. He or she need not hold a professional degree or credential in an engineering discipline. The security manager must simply be able to oversee the process of providing an integrated system solution to physical security problems. Rogers (2006) gives an excellent overview of the high-level engineering principles that security managers should apply to provide the PPS design and implementation.

This chapter focuses specifically on PPS goals and objectives and assumes some physical security is needed at a site. The goals and objectives must be met within the business strategy of the enterprise or site. Thus, the business goals and objectives of the enterprise frame the high-level PPS goals and objectives. Business elements, such as budget, time to complete, and staff availability, define the limits of what can be accomplished using a PPS, but they must be supplemented by additional specific details concerning system design and implementation.

Several key concepts must be understood before it is possible to design a system that meets the identified goals and objectives. The first key concept is that of a system. A system is a collection of products, processes, or both, combined to provide a solution to a problem or goal (Martin, 1997, p. 4.). A corollary of this concept is that systems, not components, are optimized to yield the most effective design solution to the problem (Martin, 1997, p. 4). Integration is the combination of a variety of components (such as people, procedures, and

technology) to form a system. In this case, integration includes both electrical integration (where all components receive power and are interconnected) as well as functional integration (where the functions are detection, delay, and response). It is possible to have an electrically integrated system that is not functionally integrated; such a system would be vulnerable. This theme is developed further under vulnerability assessment below and design in Chapter 2.

Closely related to the idea of a system is the systems approach to problem solving. ASIS (2012) defines *systems approach* as

a logical method for problem solving in which a comprehensive solution is developed in relation to a problem having several dimensions. A type of systems approach follows three general steps: assessment of vulnerability, implementation of countermeasures, and evaluation of effectiveness.

This is another way of describing the four phases of physical security design and evaluation.

Another key concept is risk management. One definition of risk management (ISO/IEC, 2009) is “coordinated activities to direct and control an organization with regard to risk.” Although definitions of risk management vary, they generally agree that it relies on risk assessment, which in turn relies on vulnerability assessment. In addition, all definitions include threat, asset value, and vulnerability as a part of the overall risk management process. An excellent description of risk characterization, including the technical, social, behavioral, economic, and ethical aspects, can be found in *Understanding Risk: Informing Decisions in a Democratic Society* by the National Research Council (1996).

1.2 RISK ASSESSMENT/MANAGEMENT

Risk assessment developed in the insurance industry, which defined risk in terms of annualized loss expectancy, which is the product of the potential loss from an event and the likelihood of the event. Over time, various authors (Merkhofer, 1987; Hoyland & Rausand, 2004; Haimes, 1999; and Kumamoto and Henley, 1996) have molded the insurance definition into one suitable for security systems. They define risk as an uncertain situation in which a number of possible outcomes might occur, one or more of which is undesirable. In general, *risk* refers to all the adverse outcomes that an organization wishes to avoid and is a function of the probability that such consequences will occur, their magnitude, and their imminence.

Risk assessment, a necessary part of risk management, is the process of defining how big the risk is. Risk assessment techniques may be heuristic (ad hoc), inductive, or deductive. In other words, some methods are more quantitative, others more qualitative. Each method has its strengths. For example, a quantitative approach, which requires measurable data, may

make it easier to correlate security system performance and cost. (That is, a return on investment can be demonstrated.) Qualitative techniques are often based on lists and depend on how analysts feel about the solution.

Wyss (2000) describes inductive techniques as using a bottom-up approach. Risks are identified at the beginning of the analysis rather than as a result of a systematic, deductive, top-down approach. Because the list of risks is the starting point, not the result, of the research, the approach may provide incomplete results. Focusing on scenarios may also fail to account for concurrent attacks. Event trees, which trace an initiating event through a sequence with different possible outcomes, use inductive logic to infer results. Event trees are useful, but they do not readily handle feedback loops within the system.

Deductive risk assessment uses logic diagrams to determine how a particular undesired event may occur. Fault trees are often used with event trees to determine the basic causes of the event. Also used are influence diagrams, which are often employed in computer systems. For each location, conditional probabilities are assigned to various events. Using probabilistic risk *assessment* is more formal, scientific, technical, quantitative, and objective than risk *management*, which is based on value judgment and heuristics and is more subjective, qualitative, societal, and political. Ideally, probabilities should be based on objective likelihood, but in security it is common to estimate likelihood based on subjective factors, such as intuition; expertise; partial, defective, or erroneous data; and sometimes dubious theories. These qualitative factors introduce much uncertainty. In security systems, the uncertainty is especially great because of the lack of dependable data on all types of adversary attacks. An event's likelihood and impact can be evaluated more easily when causal scenarios are used. However, not all scenarios can be anticipated.

Simulation tools (often software) are used to complement logical models. A simulation tool can help evaluate scenarios created through the logical model. Scenarios may be clustered into related groups to make their number more manageable. Scenarios may also be suggested by regulatory agencies, subject matter experts, or a history of previous incidents. Complex simulation tools may automatically generate scenarios for evaluation. Such tools much be validated before being used.

Risk assessment examines the outcome of a successful adversary attack, the likelihood it will occur, how it will unfold, and how many people will be affected. When an entire population is at risk, it is called a societal risk.

In risk assessment, the analyst attempts to answer three questions (Kaplan & Garrick, 1981):

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

Answering those questions aids in the process of identifying, measuring, quantifying, and evaluating risks.

Risk management comes next. It builds on risk assessment by answering a second set of questions:

- What can be done?
- What options are available?
- What are their associated tradeoffs in terms of costs, benefits, and risks?
- What are the impacts of current management decisions (i.e., policy) on future options?

Answering the last question leads to the optimal solution. Thus, risk management is a systematic, statistically-based, holistic process that employs formal risk assessment and management and addresses the sources of system failures. This approach can help security managers provide the right information to senior managers to help them make informed decisions.

Kaplan and Garrick devised their approach for use in a relatively quantifiable context: engineered systems. By contrast, security systems face many unpredictable elements, such as the probability of attack by all threats (human adversaries) in a statistically accurate sense. Terrorist attacks cannot be predicted reliably, though high-visibility attacks since September 11, 2001, suggests ongoing danger (London and Madrid rail bombings, Mumbai attack). On the other hand, some aspects of security are quantifiable. Management of a retail chain may know how often shoplifters attack each store in the enterprise. It is also feasible to measure an asset's value to the enterprise and to measure the performance of security technology.

In general, risk can be reduced in three ways:

- preventing an attack by detecting it before it is under way
- protecting against an attack
- reducing (mitigating) consequences

Prevention requires intelligence gathering and deterrence. Protection requires a physical protection system.

In risk analysis, mitigation means reducing consequences given the event. Mitigation focuses solely on reducing consequences. Mitigation measures may be implemented before, during, and after an attack if the measures reduce consequences. For example, lowering the level of a reservoir to reduce the consequences of a flood from a potential breach of its embankment is a mitigation measure, as is providing vaccinations before an outbreak of disease to reduce the consequences from an epidemic.

Risk management programs should include both risk financing (insurance) and risk control tools. Approaches include avoidance, reduction, spreading, transfer, and acceptance (Grose, 1987). A PPS is one subsystem in an overall strategy for reducing risk.

Risk can be described as the likelihood of a consequence (ASIS, Organizational, 2009). If it is impossible for the consequence to occur (i.e., there is no feasible way for the undesirable outcome to happen), there is no risk. However, that is an unlikely assumption given the reality of attacks. Still, if the consequence of loss or likelihood of occurrence is low, or both are low, the risk will be low. Informed decision making is the basis of risk management.

In the field, there is considerable agreement that *threat*, *consequence*, and *vulnerability* are the right terms for expressing risk (Broder, 2006, p. 41; Fisher & Green, 1998, Garcia, Vulnerability, 2006, p. 9; Kaplan & Garrick, 1981). Threat is a combination of adversary capabilities, equipment, motivation or intent, and likelihood of attack (Garcia, 2008). Likelihood of attack may be measured in terms of frequency or probability. Frequency is the number of times the undesired event happens over a period (for example, attacks per year). Probability is the likelihood of one outcome out of the total of all possible undesirable outcomes, expressed as a number between 0 and 1 (Young, 2010). Consequence is the undesirable outcome itself (Garcia, 2008). System effectiveness is the ability of the PPS to prevent a successful attack once it has been initiated. Vulnerabilities are PPS weaknesses that can be exploited by adversaries (ASIS, 2012).

To manage security risk, it is necessary to try to determine which malevolent human adversaries will try to steal or sabotage which important assets. Risk assessment helps identify threats, assets, and vulnerabilities through a systematic, defensible process. One ASIS definition (ASIS, Organizational, 2009) calls risk assessment

the overall process of risk identification, risk analysis, and risk evaluation. Note: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

After the threats and assets are defined, a vulnerability assessment is generally performed to establish a baseline of PPS effectiveness in meeting goals and objectives. These are the remaining key concepts of Part 1 of the PPS cycle, physical protection system goals and objectives. At this point, a decision must be made whether the existing PPS is meeting goals and objectives; if not, it is time to begin Part 2 of the PPS cycle, the design phase.

1.3 THREAT DEFINITION

A threat definition for the site or enterprise must be created during the risk assessment and specific information must be collected about the adversary. Adversaries can be separated into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be defined (Garcia, 2008, pp. 26-30). For any given site in an enterprise, there may be several threats, such as a criminal outsider, a disgruntled employee, terrorists, or some combination of these, and the security system must protect assets against all of these threats.

ASIS defines the design basis threat (DBT) as “the adversary against which the utility must be protected” (Patterson, 2007). Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence. This definition can be modified to include all sites, not only utilities. Key points in the threat definition require some specific details.

In this context, the threat comes from malevolent humans, not accidental (safety-related) events. While safety and security are related and complementary functions, a PPS is implemented primarily to stop malevolent attacks, not to prevent fires or respond to acts of nature or unintentional human errors (like spilling a bucket of water). It is also important to differentiate security protection from safety protection. Safety is generally defined as the measures (people, procedures, or equipment) used to prevent or detect an abnormal condition that can endanger people, property, or the enterprise. These abnormal conditions include accidents caused by human carelessness, inattentiveness, and lack of training, as well as other unintentional events. Security, on the other hand, refers to the measures used to protect people, property, or the enterprise from malevolent human threats (Garcia, Risk, 2006, pp. 510-511). Of course, a good security risk management program considers safety events since they may have the same consequence as security events.

The key distinction between security and safety events is their cause—accidental, unintentional, or natural disaster (abnormal event) versus malevolent, intentional human-caused event. Snell (2002) describes the theoretical basis for performing security and safety assessments differently.

The DBT includes other characteristics of the threat that should be considered, such as vehicles, weapons, tools, or explosives, as well as the threat’s motivation. It is critical that these characteristics are described in the DBT because later, during the vulnerability assessment (VA), they will help in gauging the effectiveness of the individual PPS components, as well as the overall system. The VA process and these effects are described further in the vulnerability assessment section below, as well as in Chapter 2, Design Principles and Concepts.

Adversaries may be motivated by ideological, financial, or personal reasons. The motivation may make a big difference in the protection system that is needed. For example, a highly motivated adversary who is willing to die for a cause is much different than vandals who will flee when discovered. It is also important to consider the number of adversaries. Proper responses cannot be designed without knowing how many adversaries are expected to attack. For example, if a site has five responders and the adversary attacks with 10, the adversary has the advantage in numbers and can be much more difficult to stop. This problem is exacerbated if the adversary has better or more weapons and equipment. In addition, for responders to train effectively, they must train to some threshold. Lacking this threshold, it is unclear how to predict a win for the responders. This example assumes there will be an immediate response to a security event; if there is no immediate response, the analysis is different. Verifying system performance against the defined threats is the basis of vulnerability assessment (Garcia, 2006, Risk, pp. 26-30).

There are various methods of defining threats to a facility (Garcia, 2008, pp. 25-39; Young, 2010, pp. 48-53; Catrantzos, 2010, pp. 8-10), and any may be used effectively as long as they provide the specific characteristics described above. An important concept is the threat spectrum. Most sites need to prepare for a variety of threats. A site may be attacked for many reasons, and attacks often focus on stealing or sabotaging an asset. The threat spectrum uses categories or labels to describe the threat characteristics for various levels of threats. Any organized method may be used to collect information and create a site's threat spectrum, but the process must result in specific characterizations, not a general listing. Many sites have used labels such as vandals, disgruntled employees (insiders), criminals, and extremists to describe their threat spectrum. While these labels may communicate some information, they are not sufficient to aid in a vulnerability assessment or in system design. The DBT is a tool that the vulnerability assessment team and system designers use to establish system requirements. A well-defined threat spectrum might look like this:

- **Vandals.** This threat would consist of a small group of two to five unarmed people, whose intent is to deface low-value company assets or employee vehicles parked on-site. Attacks are most likely at night, but daytime attacks have occurred. The vandals may be under the influence of drugs or alcohol. They may carry a few basic hand tools, such as pliers, wire cutters, screwdrivers, or hammers, as well as cans of spray paint, paintball guns, or similar items. They do not have insider assistance. They are not highly motivated and will flee or surrender if they perceive that they are about to be caught.
- **Disgruntled employee (insider).** Generally this threat would come from an individual acting alone, but there could possibly be a small group (two to five persons). The person might be under the influence of alcohol or drugs, or he or she may be mentally unstable. The person may carry small weapons, such as a pistol or knife. The disgruntled employee's desire is to attack a person at the site, such as a manager or

spouse, or to cause damage to equipment at the site. If equipment damage is the goal, the person may carry small tools but will more likely use tools or controls already on-site. The person is highly motivated and does not expect to be caught during the act, due to the person's authorized access.

- **Criminals.** These may be one to five people whose goal is theft of valuable property from the site; their goal is to gain financially by selling the stolen items. They will carry hand or power tools to enter the site or access the asset, and they will carefully plan their attack. They may carry small weapons but are unlikely to use them. They may have insider assistance and will break off the attack if detected.
- **Extremists.** This threat consists of a medium-sized to large group of people (20 and up) whose goal is to bring attention to a practice of the targeted site. Their motivation is ideological; they may be environmentalists, animal rights groups, anti- or pro-abortion demonstrators, or shareholders. They are nonviolent but may resist eviction from a site and will ignore verbal commands to leave.

The use of low, medium, or high levels to describe various threats may be used in place of the descriptive labels shown in this example. The threat spectrum above includes insiders, either as the actual threat or working with outsiders to accomplish the attack. Outsiders are those who do not have authorized access to a site (whether occasional access or everyday access). Insiders are those who have regular, authorized access and include all employees, subcontractors, and vendors, among others. Simple labels, or a limited view of the threat, may not be sufficient when identifying vulnerabilities or estimating risk. The security measures required to stop criminals are quite different from those required for stopping extremists. In the former case, a well-equipped adversary must enter the site (either the outside grounds or a building interior, depending on where assets are located), get to the item, and then leave the site to be successful. Such a threat can be addressed with a well-integrated PPS. In the case of extremists, by contrast, a PPS may not be effective, even a rudimentary system that uses fences and has posted signs prohibiting unauthorized entry. By studying the entire threat spectrum, one can design a PPS that is effective against all threats and the full range of adversary tools, weapons, and capabilities. A PPS designed this way will be more effective across the entire threat spectrum, and the appropriate equipment, procedures, and personnel will be efficiently applied to the security problem.

Once the spectrum is constructed, it forms one basis for continuing evaluation of risk and vulnerability. The DBT may consist of one level or several. Once created, the DBT should be protected as sensitive information, since it will be the basis for the evaluation of the site and could be used by a threat to determine the best way to attack.

An additional element of threat definition is estimating the likelihood that the adversary will attack. This can be highly problematic, especially in cases where there is little data to support

the estimate. As with threat definition, there are several ways to estimate the likelihood of attack (Broder, 2006, pp. 21-27; Young, 2010, pp. 81-107). For sites that have data, whether from incident reports or other sources, this estimate might be easier; at sites where an attack by a particular threat is possible but happens infrequently, or perhaps not at all, there are choices to make. It may be possible to obtain attack data regarding the area around the site, data for the relevant business sector, or various forms of law enforcement. The likelihood of attack can be a frequency, a probability, or a qualitative estimate. Frequency calculations are supported where there is considerable data available, such as in the case of shoplifting at a particular store or across an entire store network. Probabilities are similar to frequencies but are based on a more theoretical view. Qualitative estimates rank the attack possibility as very likely or highly unlikely, for example. Where there is no data to support an estimate, another approach is to assume that there will be an attack and then evaluate risk on this basis. In this case, the risk is conditional, i.e., the condition is that there will be an attack (Garcia, 2008, p. 292). Not every site has experienced a workplace violence attack, yet almost all sites include workplace violence in their threat definition.

1.4 **HISTORICAL EXPERIENCE**

A special problem exists with regard to historical experience: There are usually not enough historical data in usable form within most enterprises to permit accurate forecasting. The problem has two aspects: the availability of information about past losses or suspected losses, and the organization of that information into a format that permits statistical processing. Most enterprises maintain some loss data, chiefly in connection with insured losses. These losses are described in various claim notices and proof-of-loss reports to the insurance carrier. Most insurance departments maintain loss records in a database and have the capability to produce reports of losses in various formats. Some organizations maintain only the paper documents and the files will not yield useful history except through extensive rearrangement of data. A note of caution—the database may only contain information as of the date of inception of the database. Prior records may not have been entered. In other enterprises, where the risk of loss is either ignored (no insurance or other risk management measure) or assumed (self-insurance or very large deductibles in commercial policies), the records may not exist. That is, in many organizations, if a loss is not insured and does not come within the dollar coverage limits of the policies, records of the loss are transitory and may not be accessible over time. Accurate historical information about losses or loss events can be among the most useful information kept by an enterprise. First of all, sufficient information makes it possible to forecast future occurrences. The science of statistics shows that the frequency of occurrence suggests the probability of future recurrence. A distribution curve based on the number of times various kinds of events have occurred among other similar events indicates which events have a high probability of occurring again. (For an extended discussion, see Walsh, 1995.) Along with the

other facts developed in the probability factors evaluation, this approach can be used to arrive at an overall statement of likelihood of occurrence.

Predictions are of secondary importance, but their accuracy increases with the accumulation of historical data. It is a principle of probability theory that the larger the number of actual cases or events of the kind that includes the predicted event, the greater the agreement between the predicted pattern and the actual pattern of occurrence. For a very large enterprise, such as a commercial or industrial organization with multiple locations or a retail chain with many outlets, the volume of data available from internal collection alone could be sufficient to allow accurate predictions.

The second aspect of the historical loss information problem concerns the organization of the information. It is not unusual to find assets protection departments that keep incident or other suspicious event reports dating back many years. In the past, each report consisted of one or more sheets of paper which had to be studied individually to yield any data.

The modern assets protection department uses a database to record incidents. These databases range from complex incident management systems purchased from specialized software vendors to relatively simple database software that is provided with most computers. In many instances the information is keyed into a report screen in the database by the investigating security personnel. If manual incident report forms are used to collect the information, they are designed to simplify the input of the information into the database. Thus, codes are frequently used to denote the type of incident or the method of operation.

The database usually includes at least these fields:

- date of occurrence
- time of occurrence
- place of occurrence (pinpointed as precisely as desired, even to the post-and-column intersection of a given building area)
- nature of the event under a general head such as crime or accident
- specific description of the event, such as fire, larceny by stealth, forced entry, mysterious disappearance, etc.
- method of operation or mode of occurrence, if known (such as padlock hasp removed with pry bar, window used for entry and exit, or fictitious person named on requisition)
- number for the distinctive event, to serve as the general locator for the incident and unite all files, reports, and log data
- value of the assets involved and value of damage

The database reporting software usually provides for retrieval of the information in any desired order. The data can be viewed on the screen in detail or in summary format, or the information can be printed out. Such information has real value in vulnerability assessment. Every professional asset protection or loss prevention staff should have a system for collecting incident data suitable for the size and complexity of the enterprise.

Once the DBT is created and there is some estimate of the likelihood of an attack, it is time to move to the second key aspect of defining goals and objectives—asset identification.

1.5 **ASSET IDENTIFICATION**

Like threat definition, asset identification is critical to an estimate of risk at a site. There are several ways to approach this effort, almost all of which assign a value to the asset. This value has been described as criticality, consequence of loss (Garcia, 2008, p. 44), or severity (Fisher & Green, 1998). Regardless of the terminology, assets must be identified and prioritized in terms of the effect their loss could have on the site or enterprise. While damage to or loss of some assets may have little effect on the site (perhaps graffiti on a wall), other assets are critical to the company and have an unacceptably high consequence of loss. Examples include harm to employees due to a workplace violence incident, or loss of a proprietary formula, bid, or research and development results or equipment.

There are three general methods of valuing assets—through the use of dollars, by using consequence criteria, or by policy. Examples of valuing by dollars and criteria follow; asset valuation by policy is common at government or military sites. For example, the U.S. Air Force sets protection levels for all Air Force assets, ranging from nuclear weapons down to small appliances, such as ovens or washers and dryers. Other local, state, and federal agencies have similar policy designations for assets.

1.6 **LOSS IMPACT**

Loss impact can be measured in a variety of ways. One measure is the effect on employee morale; another is the effect on community relations. The most important measure overall is in dollars. Because the money measure is common to all ventures, even not-for-profit enterprises, the seriousness of security vulnerability can be most easily grasped if stated in monetary terms.

When the tradeoff decisions are being made as part of the risk management process, the only useful way to evaluate security countermeasures is to compare the cost of estimated losses with the cost of protection. Money is the necessary medium.

Security professionals often have difficulty achieving sufficient credibility or acceptance with enterprise management to develop an adequate program. A chief reason is the absence of quantitative evaluations of the security effort. Although social responsibility in a broad sense is a recognized part of enterprise management, most managers and senior executives still set goals and measure results in financial terms, either profit achieved or costs reduced.

To fit easily into a typical manager's frame of reference, security and assets protection programs must be cost-justified. Ignoring or underplaying cost implications while emphasizing the need for security will predictably generate low-grade programs. Cost justification means not spending more than the benefits derived are worth.

Costs to Be Considered

Costs of security losses are both direct and indirect. Direct costs include the loss of money, negotiable instruments, property, or information. Indirect costs include harm to reputation, loss of goodwill, loss of employees, and harm to employee morale. Both direct and indirect costs can be measured in terms of lost assets and lost income. Often, a single loss results in both kinds of costs.

Permanent Replacement

The most obvious cost is that involved in the permanent replacement of a lost asset. If a building is destroyed by fire, finished goods are lost through diversion, or a laptop computer is stolen from an office, the lost asset must be replaced. If the asset is a product, the proprietor may elect not to replace but to absorb the cost of production and the unrealized profit that would have been earned. Although a viable option, this course is not the one that a healthy business would choose, because failure to offer a product that could have been sold tends to have an impact on market share. If the asset is a tool of production, its replacement is even more important because it is essential to the continued activity of the enterprise.

Permanent replacement of a lost asset includes all costs to return it to its former location. Components of that cost include the following:

- purchase price or manufacturing cost
- freight and shipping charges
- make-ready or preparation cost to install it or make it functional

A lost asset may have cost significantly less when it was first acquired than a replacement would cost now. Conversely, a replacement computer might cost less than the original.

Temporary Substitute

In regard to tools of production and other items making up the active structure of the enterprise, it may be necessary to procure substitutes while awaiting permanent replacements.

This may be necessary to minimize lost sales and profit and to avoid penalties and forfeitures often encountered when a contractor fails to deliver. The cost of the temporary substitute is properly allocable to the security event that caused the loss of the asset. Components of temporary substitute cost might include lease or rental or premium labor, such as overtime or extra shift work to compensate for the missing production.

Related or Consequent Cost

If personnel or equipment cannot be used fully or at all because an asset was lost through a security incident, the cost of the downtime is also attributable to the loss event. This happens most often when the stoppage of one activity prevents other activities as well. Loss of discounts in paying bills due to failure of a computer and delay in completing the accounts payable cycle is an example.

Lost Income Cost

In most enterprises, cash reserves are held to the minimum necessary for short-term operations. Remaining capital or surplus is invested in income-producing securities. The larger the enterprise, the more important these investments are. If cash that might otherwise be so invested must be used to procure permanent replacements or temporary substitutes or to pay consequent costs, the income that might have been earned had the cash remained invested must be considered part of the loss. If income from investment is not relevant to a given case, then alternative uses of the cash might have to be abandoned to meet emergency needs. In either case, the use of the money for loss replacement represents an additional cost margin and is called lost income. One formula is as follows:

$$I = \frac{i}{365} \times P \times t$$

I = income earned

i = annual percent rate of return

P = principal amount (in dollars) available for investment

t = time (in days) during which P is available for investment

For example, the income earned from \$1,000, invested at 10 percent per annum for a period of 90 days, would be \$24.66.

Cost Abatement

Many losses are covered, at least in part, by insurance. Indeed, in some enterprises it is still the practice to consider insurance as the only factor in risk loss protection. This approach is becoming less common and is being replaced by modern risk management techniques. Risk management is an overall designator applied to the combined functions of loss prevention, loss control, and loss indemnification, typified in older business organizations by the use of engineering, fire and security, and insurance departments. Some insurance coverage, usually far from total, is available for many losses. To the extent it is available, that amount should be subtracted from the combined costs of loss enumerated above. But even where insurance is available, there is usually a purchase cost or allocable premium share connected with the particular assets for which the insurance claim is made. For precision, that cost or share should be subtracted from the available insurance before the insurance is, in turn, used to offset the cost of loss.

Cost-of-Loss Formula

Taking the worst-case position and analyzing each security vulnerability in light of the probable maximum loss for a single occurrence of the risk event, one can use the following equation:

$$K = (Cp + Ct + Cr + Ci) - (I - a)$$

K = criticality, total cost of loss
Cp = cost of permanent replacement
Ct = cost of temporary substitute
Cr = total related costs
Ci = lost income cost
I = available insurance or indemnity
a = allocable insurance premium amount

The assets protection staff does not usually have this information immediately available and must work with the financial and insurance organizations to develop it. But an enterprise with extensive insurance coverage probably has accumulated much of the information in the course of preparing schedules of coverage. It is not unusual to find extensive criticality data in an insurance department and some form of loss-risk probability data in the assets protection or security department. Far less often are these data systematically combined. Logically, however, they must be combined for either aspect of the risk management scheme to fulfill its intended purpose. When the cost data have been collected, a decision can be made as to the proper criticality.

Consequence Criteria

The use of consequence criteria is another approach to asset valuation (Garcia, 2008, p. 45). Criteria such as harm to national security, number of days to recover, number of people

harm, or damage to corporate reputation can also be used. For each criterion, one needs value ranges to help assess the value of an asset. These may be quantitative or qualitative estimates. The criteria and their ranges can then be placed in a table, the assets evaluated using the criteria, and a final, prioritized list of assets created. A sample table is shown in Figure 1-1.

| Undesired Consequence | Estimate of Loss | | |
|-----------------------|-------------------------|--------------------------|---------------------------|
| | Low | Medium | High |
| Loss of life | 1-10 | 11-50 | >50 |
| Loss of asset | <\$5K | \$5-50K | >\$50K |
| Days out of operation | <1 | 2-3 | >3 |
| Loss of reputation | Stock price drops 1 day | Stock price drops 5 days | Stock price drops 30 days |
| Redundancy | >3 locations | 2 locations | 1 location |

Figure 1-1
Sample Consequence Table

Value ranges are associated with each consequence. It is best to use quantitative criteria, as they are harder to manipulate and less likely to skew results. Only four to eight criteria should be used so the figure does not become unwieldy or the process unmanageable.

Figure 1-1 shows representative criteria, which may or may not be applicable to a given site. Appropriate consequences should be developed for the enterprise or facility, and then assets ranked accordingly. In this example, loss of life can include employees, visitors, residents in an area, or a combination of all of these. Loss of asset can be through theft or sabotage. Days out of operation can include the initial loss of production and time to recover, or time for recovery could be a separate criterion. Loss of reputation is included because this is a serious concern for many publicly traded corporations; other measures could use periodic marketing surveys, loss of sales over a period of time, or the number of negative citations in local or national newspapers or other media. Redundancy is a useful criterion for facilities that have unique assets, such as a semiconductor, chemical, or drug-process line, or large shipbuilding or oil-platform building facilities. If the line only exists in one location and it is damaged, it may take a long time to get back into operation. If, on the other hand, there are other locations that could increase output to cover the loss, the overall consequence may be lower.

At this point, there is enough information to proceed to the next step in the risk analysis, vulnerability assessment. In many situations, threats and targets for the site or enterprise have already been identified as part of an overall security risk assessment. This is an excellent example of one of the efficiencies of assessing security risks across the site. As an example, the overall risk assessment at a facility might include loss of a key trade secret. Loss of this information would be unacceptable to the company, so it must be protected. This would be true of all forms of the information, which might be in hard or soft copy. In this case, both the PPS and the cybersecurity system would need to protect the asset from the defined threat.

1.7 VULNERABILITY ASSESSMENT (VA)

Vulnerability assessment is the process of identifying and quantifying vulnerabilities. The term *vulnerability analysis*, which is a method of identifying the weak points of a facility, entity, venue, or person (ASIS, 2012), has also been used to describe this process. Both terms are acceptable and make the same point—that one must evaluate the state of the PPS at a facility to determine how well it meets the defined goals and objectives. A vulnerability has been defined as “intrinsic properties of something that create susceptibility to a source of risk...that can lead to a consequence” (ISO/IEC, 2009). Garcia (2008, p. 341) offers a simpler definition that does not confuse threat and risk: a vulnerability is a weakness that can be exploited by an adversary. The latter definition is more generic and will be used for this discussion.

It is important to note that a VA must be performed once to establish the baseline of PPS effectiveness against the defined threats; it may be repeated to verify the effectiveness of proposed upgrades and then conducted again periodically to verify that the system is performing as required. The VA may provide different results against different threats, as each element of the PPS performs differently against different threats (Garcia, 2008, p. 294). In general, a well-designed, integrated PPS is more effective against lower-level threats than higher-level threats.

1.7.1 VA TEAM

Producing a complete, accurate VA requires a team with broad experience. The team should be led by a security specialist. The team should also include a security systems engineer, response expert, data analyst, operations representatives, and subject matter experts (such as technical writers, locksmiths, explosives personnel, and legal and information systems experts). Some team members may only be required occasionally, others permanently. The team leader should be experienced in security systems design and project management. The

security systems engineer needs to understand detection, delay, and response technologies and security system integration. Response experts need to know about weapons, guard force tactics and training, contingency and emergency planning, and investigation techniques. The data analyst contributes knowledge of computer modeling to predict system performance. He or she may also be a security systems engineer, a response or delay expert, or a subject matter expert. Depending on the facility and the threats it faces, the team may also need experts in locks, explosives, and other specialized matters to assess threats and establish performance goals for the designed system. In addition, input on site operations or operational impacts of proposed changes can be gained from safety, production, legal, and other representatives.

Once the team is assembled, the first phase of the design and evaluation process can begin—determining system goals and objectives. The output of this stage should be a design basis threat or threat spectrum, as well as an understanding of all assets at the facility and their associated consequence of loss. Next a site survey should be performed to create a complete facility characterization, including a description of all current security elements. At this point, the baseline system can be analyzed to make an initial estimate of system effectiveness. If the risk value is acceptable, the existing system is satisfactory; if not, the PPS must be redesigned or upgraded to lower the risk to the facility.

1.7.2 **VA CONCEPTS**

Because the PPS is a system, the VA must take a holistic view to be truly effective at exposing weaknesses that would allow for a successful attack. The biggest mistake made when conducting a VA is to concentrate on individual PPS components and address upgrades only at that level, not at the level of the overall system. For example, a VA might note that a fence has a hole in it. This is closely followed by the recommendation that the fence be repaired, with the implication that this will result in better system effectiveness. Repairing the hole will make the fence more esthetically pleasing and present an image that the site is serious about security. However, the repair alone might not actually improve security. There can be many reasons for this. A VA that focuses on the system, not the components, will expose other factors. What if the fence is only on two sides of the facility? What if there are trees or bus stop structures close to the fence? What if water has eroded some places under the fence? What about large vans or trucks parked next to the fence? Does the fence run next to a hill that makes it easy to jump over? These are all methods of easily bypassing the fence, and none of them require great skill or much equipment. An evaluation that focused only on repairing the hole in the fence might miss other, equally likely ways to defeat the fence. These, then, are all the vulnerabilities of the fence that may be exploited by a threat during an incident. Chapter 11, Analysis of the Physical Protection System, describes how these methods of defeat can be incorporated into the VA and used to predict system effectiveness.

All PPSs have some weaknesses; therefore, there will always be some risk. The key to the VA is to thoroughly evaluate the site PPS so that all paths to the assets are equally protected, and to consider what vulnerabilities exist given the defined threats, considering their motivation, tools, competence, and knowledge (Garcia, Vulnerability, 2006, p. 1). This is why a detailed threat definition is critical to the VA and the subsequent risk assessment.

1.7.3 **VA OBJECTIVES**

The major part of a VA is facility characterization, which is the evaluation of the facility's PPS. This is generally done with a site survey. The goal of a VA is to identify PPS components in the functional areas of detection, delay, and response and gather data to estimate their performance against particular threats. The PPS is characterized at both the component and system level, and the ways the threat can defeat the PPS are documented. Data collection is essential, as accurate data are the foundation for a true analysis of the PPS's ability to meet its defined objectives.

Beginning with a facility tour, the VA team gathers information on the layout of the facility, the locations of key assets, facility operations and production capabilities, and locations and types of PPS components. PPS characterization also requires review of key documents and interviews with key facility personnel at all levels. Interviews help clarify information and generate insights into the facility's operating procedures. Testing is a particularly valuable way to evaluate PPS effectiveness. Evaluation testing may show whether personnel have the skills and abilities to perform their duties, whether procedures work, and whether equipment is functional and appropriate. Evaluation tests may be of several types, such as functional, operability, and performance tests. Functional tests verify that a device is on and performing as expected (for example, that a sensor still provides a high probability of detection). Operability tests verify that a device is on and being used properly (for example, that it is still aimed at the right location). Performance testing repeats a given test enough times to establish a measure of device capability against different threats. (For example, a sensor may be tested many times, using crawling, walking, and running modes under day, night, and varying weather conditions to test the probability of detection and nuisance alarm rate). Because performance tests are rigorous and require many repetitions, they are generally impractical during a VA. Such tests are typically performed in a lab or other facility.

The VA team also needs to identify the various states that can exist at the facility. A VA is used to establish vulnerabilities at the facility at all times (24/7/365). The team needs to determine whether the PPS is more or less vulnerable during different facility states. Otherwise, the VA will be incomplete and may lead to a false sense of security. Examples of facility states include normal operating hours, nonoperational hours, a strike at the facility, emergencies (e.g., fires or bomb threats), varying weather conditions, and shift changes. Once the project

planning is complete and protection objectives are understood, the VA team should visit the facility and start collecting data.

Detection, delay, and response are the three primary functions of a PPS. **Detection** is the discovery of covert or overt action by an adversary. Key measures of effectiveness for the detection function are (1) the probability of sensing adversary action and (2) the time required for reporting and assessing the alarm. Included in the detection function is entry control—that is, allowing entry to authorized personnel and detecting the attempted entry of unauthorized personnel and material. Measures of effectiveness for entry control are throughput, false acceptance rate, and false rejection rate. Throughput is the number of authorized personnel allowed access per unit of time, assuming all personnel who attempt entry are authorized for entrance. The false acceptance rate is the rate at which false identities or credentials are allowed entry, while the false rejection rate is the frequency of denying access to authorized personnel. Detection can also be provided by the site's response force (security officers, whether at fixed posts or on patrol). Once an alarm is initiated and reported, it is time for assessment to begin. An effective assessment system provides two types of information: whether the alarm is a valid alarm or a nuisance alarm, and key details about the cause of the alarm—what, who, where, and how many.

Delay is the second primary function of a PPS. It refers to the slowing down of adversary progress. Delay can be accomplished through such means as personnel, barriers, locks, and activated delays. Response force personnel can be considered elements of delay if deployed in fixed, well-protected positions. Delay effectiveness is measured by the time required by the adversary (after detection) to bypass each delay element. The adversary may be delayed before detection, but that delay provides little value because it does not provide additional time for response. Any use of delay before detection serves primarily as a deterrent.

The **response** function consists of actions by security officers to prevent adversary success. It consists of interruption, which means enough security officers must arrive very quickly at the right place to stop the adversary's progress. Response requires communication to the security officers of accurate information about adversary actions and officer deployment. Response effectiveness is measured by the time between receipt of a communication of adversary action and the interruption of the adversary action.

The term *deployment* describes the actions of the response force from the time it receives a communication until it is in position to interrupt the adversary. Deployment's effectiveness is measured in terms of the probability of deployment to the correct location (the adversary's location) and the time required to do so.

If a site's PPS deviates from the functional integration of detection, delay, and response, the site is likely to be more vulnerable. Such vulnerability increases the risk to the enterprise. Some PPS characteristics imply a degree of risk acceptance on the part of the organization.

Examples include the lack of an immediate response to attacks on critical assets, delay with no detection, detection of intrusions with no integrated alarm assessment, or lack of integration of multiple layers of security. The amount of protection required is a function of the value of the asset and the risk tolerance of the enterprise.

The VA team's primary job is to determine security system effectiveness (Garcia, Vulnerability, 2006, p.1). After the VA is performed, the PPS must be analyzed to ensure it meets protection objectives. Analysis should not examine each PPS feature separately but should consider that a system of features is working together (Garcia, 2008, p. 3).

After analyzing facility data, the VA team reports the results in a manner that is useful to the managers at the facility. The goal is to provide accurate, unbiased information that clearly defines the current effectiveness of the PPS, along with potential solutions if the current system is not effective. The VA report informs facility management of the state of the PPS and requests upgrades that may be needed. The VA report is also used in later projects that address the vulnerabilities and improve the PPS. Much of this effort is described in Chapter 12, Implementation of the Physical Protection System.

Reporting can be formal or informal, oral or written, and may take the form of a short overview or a longer, more detailed approach. The choice of reporting form and content is an aspect of the project agreement, generally following the conventions of the customer or facility being evaluated. Regardless of presentation and documentation style, certain content must be included to make the report understandable and useful to management of the facility. A VA report is a powerful document and should not be shared indiscriminately. Protection of the final report, as well as appropriate distribution, should be defined in the master project agreement. One organization should maintain control over the document and any sharing, even though other organizations may have copies.

At a minimum, the VA report should include a description of the facility and its primary operations or products, the defined threats and identified assets, any constraints related to the VA or the site, an overall description and observations of existing PPS components, why these observations lead to vulnerabilities, a section that shows the baseline analysis of system effectiveness, and any potential upgrades or changes that can be made to the PPS to improve performance. If upgrades are proposed, an analysis using the same tools as for the baseline should also be presented, in order to demonstrate how the changes will improve system effectiveness. The use of pictures is encouraged to emphasize key points or document vulnerabilities. Detailed information on VA reporting can be found in Garcia (Vulnerability, 2006, pp. 298-305).

After the VA report is completed, the most common response is for the facility to pursue improving the PPS if the risk is high, following the recommendations of the VA team. A VA

can be thought of as the analysis of system requirements that must occur before system design and implementation. The same characteristics that made a particular PPS weak in the first place can limit the effectiveness of any upgrades if not carefully considered. The process of improving the PPS may be quick and easy if the recommendations involve only procedural or minor equipment changes, such as replacing one type of CCTV camera with another. However, if the system requires major equipment upgrades, it will be essential to take a proper, careful approach to the upgrade design.

1.7.4 **RISK ASSESSMENT**

At this point, all the inputs required to do a risk assessment are in place. As defined above, risk assessment provides the information that answers three questions: What can go wrong? What is the likelihood that it would go wrong? What are the consequences? A VA is used to support the risk assessment by answering the first question (what can go wrong?). After all the appropriate data has been collected, a risk analysis is conducted to establish the effectiveness of the security system in protecting assets against a defined threat. System effectiveness varies with the threat. As the threat capability increases, performance of individual security elements or the system as a whole will decrease. This is why a risk analysis that considers the entire threat spectrum must be performed.

System effectiveness, which is a measure of system vulnerability, is combined with threat and asset value to determine the baseline risk. If the risk is acceptable, the VA team documents the results and archives the report for future reference. If risk is not acceptable, options must be proposed to address the identified risk.

Two basic analysis approaches are used in a VA—compliance- and performance-based (Garcia, Vulnerability, 2006, p. 22). Compliance-based approaches depend on conformance to specified policies or regulations; the metric for this analysis is the presence of the specified equipment and procedures. Performance-based approaches, on the other hand, actually evaluate how each element of the PPS operates and what it contributes to overall system effectiveness. The use of compliance (or feature-based) systems is only effective against low threats, when assets have a low consequence of loss, or when cost-benefit analyses have been performed that document that physical protection measures are not the most cost-effective risk management option. A compliance-based analysis is easier to perform because the measure of system effectiveness is simply the presence of prescribed PPS equipment, procedures, and people. The analysis consists of a review of facility conformance to the compliance requirements, the use of checklists to document presence or absence of components, and a deficiency report that notes where the facility is out of compliance. The VA report summarizes these findings, and the facility makes improvements according to enterprise policy. Many sources of checklists exist and may be modified for use at a

particular site (e.g., Hess & Wroblewski, 1996). The underlying premise of a performance-based approach is that overall system effectiveness is the goal of a VA, and that all dollars spent on PPS elements should result in improved protection while also complying with requirements. Performance-based analysis techniques are recommended.

The same six-step process is used in both qualitative and quantitative performance-based analysis:

1. Create an adversary sequence diagram for all asset locations.
2. Conduct a path analysis.
3. Perform a scenario analysis.
4. Complete a neutralization analysis, if appropriate.
5. Determine system effectiveness and risk.
6. Develop and analyze system effectiveness upgrades if risk is not acceptable.

These steps are described more fully in Chapter 11, Analysis of the Physical Protection System. For now, it is sufficient to note that risk captures the relationship among threats, asset value, and system effectiveness, and is often shown in this form:

$$R = T \times A \times V$$

R = residual risk

T = threat, a combination of threat definition and likelihood of attack

A = asset to be protected

V = vulnerability, represented by system effectiveness

After the residual risk is calculated, it is included in the VA report and presented to senior management. At that point, the decision falls to management whether to accept the risk or to fund PPS upgrades.

This section described the process for establishing PPS goals and objectives. These objectives include threat definition, asset identification, and establishing acceptable risk levels to facilitate system design or before equipment is purchased. Risk is estimated through the use of a vulnerability assessment, and each enterprise must determine how much risk is acceptable. In addition, the key concepts of a system view, rather than a component view, and system integration were explained. Processes for threat definition and asset valuation were provided, and an overview of vulnerability assessment was described. The basic risk analysis process was also introduced.

REFERENCES

- ASIS International. (2012). International glossary of security terms. Available: www.asisonline.org/library/glossary/index.xml [2012, April 12].
- ASIS International. (2009). *Facilities physical security measures guideline*. ASIS SPC.1-2009. Alexandria, VA: ASIS International.
- ASIS International. (2009). *Organizational resilience: Security, preparedness, and continuity management systems—Requirements with guidance for use—American national standard*. ASIS GDL FPSM-2009. Alexandria, VA: ASIS International.
- Broder, J. F. (2006). *Risk analysis and the security survey*, 3rd ed. Boston, MA: Butterworth-Heinemann.
- Catrantzos, N. (2010). *Tackling the insider threat*. Alexandria, VA: ASIS Foundation.
- Fisher, R. J., & Green, G. (1998). *Introduction to security*, 6th ed. Boston, MA: Butterworth-Heinemann.
- Garcia M. L. (2006). Risk management. In M. Gill (Ed.), *The Handbook of Security*. New York, NY: M, Palgrave MacMillan.
- Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Boston, MA: Elsevier.
- Garcia, M. L. (2008). *The design and evaluation of physical protection systems*, 2nd ed. Boston: Butterworth-Heinemann.
- Grose, V. L. (1987). *Managing risk: Systematic loss prevention for executives*. Arlington, VA: Omega Systems Group.
- Haimes Y. Y. (1999). Risk management. In A. Sage & W. Rouse (Eds.), *Handbook of systems engineering and management*. New York, NY: John Wiley & Sons.
- Hess, K., & Wroblewski, H. (1996). *Introduction to private security*, 4th ed. Minneapolis/St. Paul: West Publishing.
- Hoyland, A., & Rausand, M. (2004). *System reliability theory* (2nd ed.). Hoboken, NJ: John Wiley & Sons.
- ISO/IEC. (2009). ISO/IEC guide 73:2002: Risk management—vocabulary—guidelines for use in standards. Geneva: ISO.
- Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk analysis*, Vol. 1, No.1.
- Kumamoto, H., & Henley, E. J. (1996). *Probabilistic risk assessment and management for engineers and scientists*, 2nd ed. Piscataway, NJ: IEEE Press.
- Martin, J. N. (1997). *Systems engineering guidebook: A process for developing systems and products*. Boca Raton, FL: CRC Press.

- Merkhofer, M. W. (1987). *Decision science and social risk management*. Dordrecht, Holland: Kluwer Academic Publishers Group.
- National Research Council. (1996). *Understanding risk: Informing decisions in a democratic society*. Washington, DC: The National Academies Press.
- Patterson, D. G. (2007). *PSP study guide*. ASIS PSPSG 2007. Alexandria, VA: ASIS International.
- Rogers, B. (2006). Engineering principles for security managers. In *The handbook of security*, Martin Gill (Ed.). New York, NY: Palgrave MacMillan.
- Walsh, J. (1995). *Risk management manual*, Vol. 1, Exposure identification. Los Angeles, CA: POA Publishing.
- Wyss, G. D. (2000). Risk assessment and risk management for energy applications. In P. Catania (Ed.), *Energy 2000: State of the art*. L'Aquila, Italy: Balaban Publishers.
- Young, C. S. (2010). *Metrics and methods for security risk management*. Burlington, MA: Syngres.

PART II

PHYSICAL PROTECTION SYSTEM DESIGN

This section describes the high-level design principles and concepts that lead to an effective PPS. As noted in Chapter 1, the process is based on the goals and objectives of the PPS, specifically considering the threat and assets at a site. Chapter 1 also defined the primary functions of a PPS as detection, delay, and response, and listed deterrence as a secondary function. Part II describes each function in more detail, examining the criteria used to select technologies and integrate them with personnel and procedures to meet system objectives.

Improper component selection, installation, maintenance, operation, and system integration are the biggest causes of vulnerabilities in a PPS. These factors are exacerbated by improper or limited training of operations or maintenance personnel, as well as ineffective or nonexistent procedures.

Part II, Physical Protection System Design, is organized as follow:

**PART II
DESIGN**

| | | |
|-------------------|-------------|-----------------------------------------------|
| | Chapter 2. | Design Principles and Concepts |
| DETERRENCE | Chapter 3. | Crime Prevention Through Environmental Design |
| DETECTION | Chapter 4. | Sensors |
| | Chapter 5. | Video Subsystems and Alarm Assessment |
| | Chapter 6. | Lighting |
| | Chapter 7. | Alarm Communication and Display |
| | Chapter 8. | Entry Control |
| DELAY | Chapter 9. | Delay Barriers |
| RESPONSE | Chapter 10. | Response |

Part II. Summary

CHAPTER 2

DESIGN PRINCIPLES AND CONCEPTS

The effectiveness of the PPS functions of detection, delay, and response and their relationships have been discussed. In addition, all of the hardware elements of the system must be installed, maintained, and operated properly. The procedures of the PPS must be compatible with the facility procedures and integrated into the PPS design. Training of personnel in policies, procedures, and operation of equipment is also important to system effectiveness. Security, safety, and operational objectives must be accomplished at all times.

2.1 PPS CHARACTERISTICS

A well-engineered PPS exhibits the following characteristics:

- protection-in-depth
- minimum consequence of component failure
- balanced protection

2.1.1 PROTECTION-IN-DEPTH

Protection-in-depth means that to accomplish the goal, an adversary should be required to avoid or defeat a number of protective devices in sequence. For example, an adversary might have to defeat one sensor and penetrate two separate barriers before gaining entry to a process control room or a filing cabinet in the project costing area. The actions and times required to penetrate each of these layers may not necessarily be equal, and the effectiveness of each may be quite different, but each will require a separate and distinct act by the

adversary moving along the path. The effect produced on the adversary by a system that provides protection-in-depth will be

- to increase uncertainty about the system,
- to require more extensive preparations prior to attacking the system, and
- to create additional steps where the adversary may fail or abort the mission.

2.1.2 **MINIMUM CONSEQUENCE OF COMPONENT FAILURE**

It is unlikely that a complex system will ever be developed and operated that does not experience some component failure during its lifetime. Causes of component failure in a PPS are numerous and can range from environmental factors (which may be expected) to adversary actions beyond the scope of the threat used in the system design. Although it is important to know the cause of component failure in order to restore the system to normal operation, it is more important that contingency plans are provided so the system can continue to operate. Requiring portions of these contingency plans to be carried out automatically (so that redundant equipment automatically takes over the function of disabled equipment) may be highly desirable in some cases. An example of this is the presence of backup power at a facility. In the event that an adversary disables the primary power source, generators or batteries can be used to power the security system. Some component failures may require aid from sources outside the facility to minimize the impact of the failure. One example of this is the use of local law enforcement to supplement airport security personnel at times of higher alert status. In this case, the component failure is the temporary lack of sufficient response forces under new threat conditions.

2.1.3 **BALANCED PROTECTION**

Balanced protection means that no matter how an adversary attempts to accomplish the goal, effective elements of the PPS will be encountered. Consider, for example, the barrier surface that surrounds a room. This surface may consist of the following:

- walls, floors, and ceilings of several types
- windows and doors of several types; equipment hatches in floors and ceilings
- heating, ventilating, and air conditioning openings with various types of grilles

For a completely balanced system, the minimum time to penetrate each barrier would be equal, and the minimum probability of detecting penetration of each of these barriers should be equal. However, complete balance is probably not possible or desirable. Certain elements, such as walls, may be extremely resistant to penetration, not because of physical protection

requirements, but due to structural or safety requirements. Door, hatch, and grille delays may be considerably less than wall delays and still be adequate. There is no advantage in overdesigning by installing a costly door that would take several minutes to penetrate with explosives, if the wall surrounding the door is standard drywall, which could be penetrated in a few seconds with hand tools.

Finally, features designed to protect against one form of threat should not be eliminated because they overprotect against another threat. The objective should be to provide adequate protection against all threats on all possible paths and to maintain a balance with other considerations, such as cost, safety, and structural integrity.

2.2 DESIGN CRITERIA

Any design process must have criteria against which elements of the design will be evaluated. A design process based on performance criteria will select elements and procedures according to the contribution they make to overall system performance. The effectiveness measure will be overall system performance. By establishing a measure of overall system performance, these values may be compared for existing (baseline) systems and upgraded systems and the amount of improvement can be determined. This increase in system effectiveness can then be compared to the cost of implementation of the proposed upgrades and a cost-benefit analysis can be supported.

A feature criteria approach selects elements or procedures to satisfy requirements that certain items are present. The effectiveness measure is the presence of those features. The use of a feature criteria approach in regulations or requirements that apply to a PPS should generally be avoided or handled with extreme care. The feature criteria approach can lead to the use of a checklist method to determine system adequacy, based on the presence or absence of required features. This is clearly not desirable, since overall system performance is of interest, rather than the mere presence or absence of system features or components. For example, a performance criterion for a perimeter detection system would be that the system be able to detect a running intruder using any attack method. A feature criterion for the same detection system might be that the system includes two specific sensor types, such as motion detection and a fence sensor.

The conceptual design techniques presented in this text are based on a performance-based approach to meeting the PPS objectives. Much of the component technology material will, however, be applicable for either performance criteria or feature criteria design methods.

The performance measures for the PPS functions are:

- Detection
 - Probability of detection
 - Time for communication and assessment
 - Frequency of nuisance alarms
- Delay
 - Time to defeat obstacles
- Response
 - Probability of accurate communication to response force
 - Time to communicate
 - Probability of deployment to adversary location
 - Time to deploy
 - Response force effectiveness

2.3 ADDITIONAL DESIGN ELEMENTS

An effective PPS combines people, procedures, and equipment into an integrated system that protects assets from the expected threat. The personnel and technology components are often emphasized, yet the value of procedures as protection elements cannot be overstated. Procedural changes can be cost-effective solutions to physical protection issues, although when used by themselves they will only protect assets from the lowest threats. Procedures include not only operational and maintenance procedures but also the training of facility personnel in security awareness and of security officers or other response forces in when and how to stop an adversary. Another procedural design tool is the use of investigations. Investigation may be the response to a loss event or may be used to anticipate a threat, such as in background investigations of potential employees. Regardless of how the investigation tool is used, it is an important design element in a PPS and should be used when appropriate. Of course, for critical high-consequence loss assets, an investigation after the fact may be too late. In these cases, more immediate responses will be required to prevent loss of or damage to the critical asset.

In addition to use of the investigative tool, some corporations are applying more resources to the use of technical surveillance countermeasures, such as sweeps and searches for electronic bugging devices. This is an additional aspect of a security system that, like executive protection, must be part of an integrated approach to asset protection. The use of hotels and other nonproprietary sites for seminars or meetings provides the opportunity for

industrial espionage. For these threats, a security manager may choose to send personnel to the meeting location and ensure that a room or area is free of any recording or other surveillance equipment. Technical surveillance techniques may also be used within a facility, either on a daily basis or for some special events, such as on-site board of directors meetings, to prevent theft of information.

The performance measures for investigative and technical surveillance techniques do not lend themselves to quantification as readily as technical protection elements. In these cases, discovery of the person responsible for the theft or damage or the presence of surveillance devices serves as the measure of performance for the design element. These tools are very useful but may not be sufficient for protection of critical assets at sites. As with any design, the design elements used to achieve the protection system objectives will depend on the threat, the likelihood of an attack, and the consequence of loss of the asset.

Many different procedural elements can be incorporated into an effective system design at a facility. Procedures can supplement a good technical design and training. Procedures that can be considered, depending on the threat and the value of the asset, include shredding of all papers before disposal, locking procedures for safes, password control and update for computer systems, random drug searches in accordance with company policies and legal requirements, periodic audits of employee computer files, and issuing parking permits to employees and authorized visitors.

As was noted earlier, deterrence is a secondary function of a PPS and will be discussed next, followed by discussion of the three primary functions: detection, delay, and response.

PPS FUNCTION

DETERRENCE

Theft, sabotage, and other malevolent acts at a facility may be prevented by deterring the adversary or by defeating the adversary. Deterrence is achieved through measures that potential adversaries perceive as too difficult to defeat; it makes the facility an unattractive target so the adversary abandons or never attempts an attack. Examples of deterrents are security officers in parking lots, adequate lighting at night, signs, and barriers, such as bars on windows. Deterrence features discourage some adversaries, but they are not necessarily useful defenses against an adversary who chooses to attack anyway.

The level of deterrence provided by a PPS is difficult to measure. A PPS cannot be deemed effective simply because an adversary has not yet challenged the system. Because relying on deterrence is risky, deterrence is considered a secondary function of a PPS.

As more research on the long-term value of deterrents is completed, specific deterrents may be incorporated into protection system design. To date, however, there is no statistically valid information to support the effectiveness of deterrents. The perceived likelihood of detection and the expected severity of punishment are certainly factors in deterrence, yet some employees feel they will never be caught, so deterrence cannot be relied on. Deterrence may serve as a first line of defense, but if an asset's value is high enough, further measures will be needed. While some threats may be deterred, not all threats will.

The following chapter, addressing crime prevention through environmental design, describes one important approach to the deterrence function.

CHAPTER 3

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN

3.1 CPTED THEORY

Since the 1970s, the term *crime prevention through environmental design* (CPTED, pronounced “sep-ted”) has become the preferred way to describe the following security concept:¹

The proper design and effective use of the built environment can lead to a reduction in the opportunity, fear, and incidence of predatory stranger-to-stranger type crime, as well as result in an improvement of the quality of life (of where and how we live, work, and play).

CPTED is the design or redesign of a venue to reduce crime opportunity and fear of crime through natural, mechanical, and procedural means. CPTED is a crime prevention theory grounded in environmental criminology—namely, the proposition that carefully designed places such as buildings, parks, parking lots, and other structures in the surrounding environments can improve the quality of life by deterring opportunities for crime and reducing the fear of crime. As such, it also supports an improved security/asset protection posture and security awareness for the organization and/or facility where it is implemented.

At its core, CPTED is based on common sense and a heightened awareness about how people use their space for legitimate and criminal intentions. CPTED is best applied using a multidisciplinary approach that engages planners, designers, architects, landscapers, law enforcement, security professionals and facility users (residents, employees, etc.) in working teams. Security and crime prevention practitioners should have a thorough understanding of

¹ The term *CPTED* was first used by C. Ray Jeffery in his book *Crime Prevention Through Environmental Design* (Thousand Oaks, CA: Sage Publications, Inc., 1971). Later Tim Crowe used it in his book *Crime Prevention Through Environmental Design* (Boston: Butterworth-Heinemann, 1991). The CPTED definition given here is used by the National Crime Prevention Institute and was enhanced by Randall Atlas in his book *21st Century Security and CPTED* (Boca Raton, FL: Taylor & Francis Publisher, 2008).

CPTED concepts and applications to work effectively with local crime prevention officers, security professionals, building design authorities, architects and design professionals, and others when designing new or renovating existing properties.

The rising importance of CPTED in the design and planning process is based on the belief that preventing crime and losses is inherent in many human functions, behaviors, and activities and is not just something that police or security professionals do. What one does—right or wrong—with human and physical resources produces a lasting legacy. Once a property is built, it is much more difficult and expensive to make structural changes for security purposes.

For the security professional, CPTED is a set of management tools targeting the following:

- **Places.** Physical environments (such as office buildings, parking garages, parks and public spaces, multifamily apartment buildings, warehouses, schools, houses of worship and shopping centers) can be designed to produce behavioral effects that reduce the opportunity for certain types of crime and the fear of those crimes.
- **Behavior.** Some locations seem to create, promote, or allow criminal activity or unruly behavior while other environments elicit compliant and law-abiding conduct.
- **Design and use of space.** Redesigning a space or using it more effectively can encourage desirable behavior and discourage crime and related undesirable conduct.

CPTED is congruent with the security mission of deterring, detecting, and delaying likely offenders.

3.1.1 **CPTED FUNDAMENTALS**

CPTED addresses the design of physical space to support the legitimate and intended users of the space and minimize the predictable behavior of offenders. Tim Crowe (1991) refined Newman's ideas and categorized CPTED solutions as follows:

- **Mechanical measures.** Also referred to as target hardening, mechanical measures include physical security hardware and technology (such as locks, security screens on windows, fencing and gating, key control systems, intrusion detection, video surveillance, and barriers).
- **Human and organizational measures.** These include Block Watch, Neighborhood Watch, security officer patrols and posts, police officer patrols, concierge stations, building lobby bellmen, and any person or group serving as a capable guardian with the ability to observe, report, and intervene.

- **Natural measures.** Natural CPTED measures employ good space planning to reduce inhabitant conflicts by considering compatible circulation patterns. Natural measures include having a well-defined building entrance and arranging courtyards, patios, and porches for unobstructed lines of sight. Natural measures provide specific guidance for the use of space; examples include architectural landscaping, ditches, berms, bollards, planters, moats, and visibility-enhancing actions such as lighting and shrub and tree trimming. Even when supplied by mechanical equipment (lamps), lighting is classified as a natural surveillance component.

Those measures are applied with several concepts in mind:

- **Natural access control.** The idea is to employ both real and symbolic barriers—including doors, fences, and shrubbery—to define and limit access to a building or other space. For example, to deter burglars from entering lower-story windows, one could plant dense, thorny bushes near the windows or install window locking devices or an alarm system.
- **Natural surveillance.** Increasing visibility by occupants and casual observers increases the detection of trespassers or misconduct at a facility. For instance, if a high wooden fence blocks the view of a loading dock, the lack of visibility may invite thieves. Conversely, the use of chain-link fencing that allows an unobstructed view of the area by workers or passers-by may discourage thieves. Windows, door viewers, mirrors, and other design feature that improve visibility fall under natural surveillance.
- **Natural territorial reinforcement.** This is the process of establishing a sense of ownership, responsibility, and accountability in property owners, managers, or occupants to increase vigilance in identifying trespassers. For example, the use of small edging shrubbery along sidewalks in an apartment complex marks the territory of individual apartments and discourages trespassers from cutting through. Also, people pay more attention to and defend a particular space if they feel psychological ownership of it. Territorial reinforcement measures, which may be physical or symbolic, tell people they are in a defined space. Color, texture, surface variations, signage, and wayfinding systems are all part of territoriality and boundary setting. Thus, it is possible, through real barriers (fences and walls) and symbolic markers (warning signage, low hedges, low wood picket fences) to encourage tenants or employees to defend the property from individuals with undesirable intentions. Such reinforcement is termed natural because it results from normal, routine use of the environment.

In addition to the preceding classic principles, the following concepts are also considered in CPTED:

- **Management and maintenance.** For spaces to look well cared for and crime-free, they must be maintained. The “broken windows” theory (Wilson & Kelling, 1982) suggests that leaving broken windows or other decay markers (e.g., graffiti, trash, or abandoned furniture) unattended or unrepaired can lead to the impression of abandonment and increase crime opportunity as no capable guardian is observed. A parked car left too long with one broken window may soon have more. Maintenance of a building, including lighting, paint, signage, fencing, walkways, and any broken items is critical for showing that someone cares about the building and is responsible for the upkeep.
- **Legitimate activity support.** Some places are difficult to protect by nature of their location or other geographic features. In such instances, legitimate activity support is essential. A crime hotspot might be eradicated if police placed a substation there or maintenance staff moved to occupy the space, providing legitimate activity support. Drug and other criminal activity thrives in spaces that residents and management fail to claim through legitimate activities.

After gaining an understanding of natural access control, natural surveillance, territorial reinforcement, management and maintenance, and legitimate activity support, a security manager or other interested party can better address community disorder, workplace violence, street crime, and acts of terrorism. Crowe (1991) notes that CPTED solutions should be integrated with the function of the buildings or at least with the location where they are being implemented.

The application of these concepts differentiates CPTED from traditional target-hardening and fortressing techniques. Allowing CPTED concepts into initial consideration of the space configuration and circulation patterns of people, vehicles, materials and even information provides considerable efficiency advantages over retrofitting a site for security. In many instances, target hardening without consideration for the built environment creates a fortress effect, leaving residents or users feeling unsafe and isolated.

The target-hardening approach is typically not architecturally or aesthetically pleasing and usually results in resistance. To be effective, a crime prevention program must engage the stakeholders, especially residents (or employees), in identifying CPTED strategies for specific places that are defined, designated, and designed (known as the 3-D concept) for specific activities.

Graphics and Signage for CPTED

An environment or building sends messages about its designated use. Graphics and signage are among its means of communication.

A graphic is a symbol that conveys a message pictorially (e.g., the symbol of a man at a men's toilet). Signage refers to conveying a message with letters or words. Sometimes security signage puts users of a space on notice, attempting to shift some responsibility back to them. To do so successfully, the building must clearly state the expectations or ground rules, such as the following:

- Do not walk on the grass.
- Enter at own risk.
- Lock your valuables.
- No trespassing.
- Don't even think of committing a crime.

Signage may also tell users how to behave. For example, in a parking garage, signage and graphics tell users about entrances and exits, speed bumps, speed limits, direction of traffic, importance of locking up valuables, parking direction, management's lack of responsibility for losses, use of video surveillance, fire exits and alarms, and panic buttons and intercoms for assistance. Of course, just putting up a sign does not relieve the building owner of liability.

Finally, signage and graphics can help direct people to designated locations or the appropriate area of a building/compound (especially in multi-tenant facilities). This is not only helpful to facility users, but reduces "wandering" by people who may not be familiar with the property or who have nefarious intentions. It simultaneously supports a welcoming and helpful atmosphere while enhancing security and privacy for other occupants of the facility. The same can be accomplished with a properly located information kiosk or concierge/receptionist.

Several categories of considerations affect the use of security signage and graphics:

- **Architectural design considerations.** The architect or graphics consultant can offer advice about such issues as the size and typeface of letters, distance from which graphics can be read, reflectivity, necessary lighting, location, and parties intended to observe the signs and graphics. For example, for a sign to be clearly read by a person with 20/20 vision at 50 ft. (15 m), the letters must be at least 6 in. (15 cm) high, and graphics or symbols must be at least 15 in. (38 cm) high. Some typefaces are easier than others to read at a distance. Lighting levels should be at least 20 foot-candles (215 lumens per square meter), and lamps must be positioned to avoid glare on the signage.

- **Systems considerations.** Graphics and signage should be consistent, uniform, and well distributed. Just as fire exit signs must be displayed and illuminated at all stairways, security signage should be systematically displayed at all critical areas.
- **Procedural considerations.** Graphics and signage can be used to clarify procedures—e.g., having employees wear ID badges for clearance, letting guests of a restaurant know of a change in floor level, or putting shoppers on notice of shoplifting surveillance. Signs can also identify “public” areas of a facility where sensitive information should not be discussed, for example.

Graphics and signage can make people aware of the designated uses of and behaviors in an environment. If the users or invitees do not follow the rules, then the burden of responsibility shifts, and they can be challenged as to their intent. Without the notice given by signage, people’s actions are subject to personal interpretation and are difficult to challenge. Early input from the architect can help a security manager best employ signage and graphics.

3.1.2 **HISTORY OF CPTED**

The first widely published studies of crime and the environment were done in the 1920s by a group of University of Chicago sociologists (Robert Park, Ernest Burgess, Clifford Shaw, and Henry McKay). The researchers viewed the social disorganization or lack of community control found in specific inner city districts as generating high crime rates, decreasing in concentric circles away from the central business district. In making this case, they rejected the tenets of early criminological theory, which focused on the characteristics of individuals as causal agents in crime.

Later, urban planner Jane Jacobs developed concepts about “eyes on the street” and proper land use that led to the creation of the defensible space theory. She suggested that residential crime could be reduced by orienting buildings toward the street, clearly distinguishing public and private domains, and placing outdoor spaces near intensively used areas. Her book *The Death and Life of American Cities* (1961) gave police and planners an awareness of the value of natural surveillance as a crime prevention tool.

However, CPTED as it is embodied today got its start in 1973 from the early writings of Oscar Newman, who published a study of residential areas and how they contribute to victimization by criminals. His book *Defensible Space: Crime Prevention Through Urban Design* (1973) explored human territoriality, natural surveillance, and the modification of existing structures to reduce crime. Newman argued that physical construction of a residential environment could elicit behavior from residents that would, itself, contribute significantly toward their security. Appropriate building design and grouping can help inhabitants police the area themselves.

Defensible space releases tenants' latent attitudes about territorial control, allowing them to adopt behaviors necessary to protect their rights and property. The term defensible space comprises a range of mechanisms, real and symbolic barriers, strongly defined areas of influence, and improved opportunities for surveillance that combine to bring the environment under the control of its residents. Newman's work became the foundation for CPTED.

From 1973 to 1975 in the United States, the Law Enforcement Assistance Administration funded to the Westinghouse Electric Corporation to study four CPTED demonstration projects. These included a school in Broward County, Florida; a commercial corridor in Portland, Oregon; residential projects in Hartford, Connecticut, and Minneapolis, Minnesota; and a mass transportation center in Washington, DC.

The research maintained Newman's territoriality and surveillance themes but also addressed social factors. Westinghouse researchers asserted that residents needed to participate in bringing about physical and operational changes that could serve as crime prevention measures.

In *Environmental Criminology*, Paul and Patricia Brantingham (1981) argued, "Individual criminal events must be understood as confluences of offenders, victims or criminal targets, and laws in specific settings at particular times and places." Around the same time, Ronald Clarke, head of crime prevention research at the UK Home Office, empirically tested many key CPTED tenets, such as defensible space, displacement, and diffusion of benefits.

In 1994, the U.S. Department of Housing and Urban Development funded a technical assistance and training program on CPTED. Severin Sorensen was contracted to write a CPTED curriculum. Working with Clarke, he incorporated the academic and practical lessons learned since Jacobs, Newman, Crowe, and others. The resulting manual and curriculum were used until 2002.

In 1996, the International CPTED Association (ICA) was formed; among other activities, it provides a CPTED practitioner certification program.

Today, law enforcement-directed crime prevention programs exist at every level of government in the United States and Canada, largely modeled after the approach developed and institutionalized by police in the United Kingdom. CPTED work continues to be performed in academic sociology, criminology, and architecture departments; associations (e.g., National Crime Prevention Council and ASIS International); and online resources (e.g., the LinkedIn CPTED group).

CPTED has bloomed into an academic discipline with four main schools of thought: the Florida school, Australian/UK school, and eastern and western Canadian schools. Each school holds to the three first principles of CPTED (access control, natural surveillance, and territoriality), but they diverge on other issues.

3.1.3 **CRIME PREVENTION ASSUMPTIONS**

Applying CPTED requires an understanding of basic crime prevention theory and practice. NCPI (the National Crime Prevention Institute at the University of Louisville in Kentucky) has established several crime prevention operating assumptions that apply to CPTED:

- Potential victims and those responsible for their safety must be assisted to take informed actions to reduce their vulnerability to crime.
- The actions potential victims can take to prevent crime are limited by the control they can exert over their environment.
- Emphasis must be given to the environment of the potential victim rather than that of the potential criminal.
- Crime prevention is practical, not moralistic, reducing criminal motivation by reducing opportunities to commit crime.
- The punishment capabilities of courts and prisons, police apprehension, etc., can increase the risk perceived by criminals and have a significant, but secondary, role in criminal opportunity reduction.
- Law enforcement agencies should have a primary role in the reduction of crime by providing crime prevention education, guidance, and information to the public, institutions, and other community organizations, but due to budget considerations and prioritization of department resources, law enforcement agencies are primarily involved in the after-the-fact solving and apprehension of criminals, not the prevention of crime.
- Crime prevention can be both a cause and an effect of efforts to revitalize a community.
- Crime prevention knowledge is continually developing and is interdisciplinary in nature; practitioners should continually analyze successful practices and emerging technologies and share their findings.
- Crime prevention strategies should focus on the act, not the perpetrator.
- Crime prevention strategies must remain flexible and creative. What works in one situation may not work in a situation that is largely similar but that has different cultural, environmental, and other characteristics.

3.1.4 CONTEMPORARY THINKING ON CRIME AND CRIMINALS

A site's physical features may influence offender choices by altering the chances of detection or changing other factors. According to the New Zealand Ministry of Justice (2005), crime and antisocial behavior are more likely to occur under the following conditions:

- Pedestrian routes are poorly lit, indirect, and away from traffic.
- Streets, footpaths, and alleyways provide access to the rear of buildings.
- It is easy for people to become lost or disoriented.
- Criminals can operate and travel to and from the location without fear of being seen.
- Criminals and their activity do not attract attention, or criminals are confident no action will be taken.
- The sides of a building and its surrounding spaces are not easily viewed by nearby users or passersby.
- Buildings and spaces are not designed to allow surveillance outside from inside and vice versa.
- Buildings, streets, and spaces are laid out in ways that allow criminals to move around and operate undetected.
- A place brings together both people who are likely to offend and suitable targets.
- Places become derelict or underused and lack natural surveillance.
- Building entrances and exits and access to assistance are not clearly indicated.
- An area is either very quiet or very busy, depending on the local context and the type of crime.
- Groups of people feel there is nothing to do.
- Places become devoid of activity at certain times of day or night, while remaining accessible to offenders.
- It is unclear whether a space is public or private and what behavior is expected.
- Private space is easily accessible to people who have no right to be there.
- A place feels as if it is not under the supervision of local residents, businesses, organizations, or other users.
- Places are untidy or unattractive, giving the impression that they are not being cared for or that crime and disorder are tolerated.
- Signs of disorder and neglect, such as broken windows, abandoned vehicles, or graffiti, are not removed at the earliest opportunity.

- An organized human presence, such as police, security officers, or street guardians, is absent.
- The target hardening measures (e.g., for doors, windows, and gates) are inadequate for the building and the crime risk faced or are not integrated, installed, or used properly.
- There is no indication of mechanical or organized surveillance.

In short, the likelihood of crime increases when a potential criminal feels the chances of detection and identification are low and the chances of escape are high.

A study of teenage robbers (Erikson, 2003) found that the most important thing they looked for was an escape route, followed by money. Cameras and unarmed officers made little difference to them. They believed they could virtually do anything with a partner and a gun. They committed especially violent types of robberies, including street muggings, carjackings, and home invasions. Many of them did not drive because they were too young to be licensed. Sixty percent lived within two miles of the site they robbed, while only 40 percent of adult robbers lived that close to their victims. The greatest deterrence came from bullet-resistant barriers, armed officers, frequent police patrols, revolving doors, alarm systems, metal detectors, fences that block escapes, good visibility, and good lighting. Almost one-third of the adult and teenage robbers acknowledged that something at the site kept them from committing the robbery.

Target Selection

Research has found a relationship between repeat victimization, hot spots, and repeat offenders (Weisel, 2005). CPTED measures can reduce the opportunity presented by the victims and targets most likely to be victimized. Repeat victimization reflects a successful initial offense, target information gained from that experience, and use of that information to reoffend.

Some targets are especially attractive to criminals or particularly vulnerable to crime. In such cases, different offenders repeatedly victimize the victim or target. Some locations, such as corner properties, may have higher victimization because offenders can easily determine if no one is home. Similarly, ground floor apartments are more vulnerable to sliding glass door break-ins. Some businesses, such as gas stations and convenience stores, are easily accessible and are open late with few customers, increasing their exposure to robbery (Weisel, 2005).

Repeat victimization occurs in high-crime areas. Persons and places there face a greater risk for initial victimization for many crimes, and they may lack the means to block subsequent offenses by improving security measures and doing so quickly. In high-crime areas, crime is

so concentrated among repeat offenders that recurring offenses can create hot spots, or relatively small geographic areas in which offenses are clustered. CPTED can be applied to these crime hot spots to increase the difficulty of committing offenses and to increase the risks of being detected and arrested (Weisel, 2005).

At first, CPTED measures should focus on preventing the most severe acts and protecting the most frequently victimized persons and locations. The following are some steps for preventing repeat victimization (Weisel, 2005):

- **Quickly remove signs of victimization.** It is important to remove or repair obvious signs of property damage as quickly as possible. Victims may need assistance in making those repairs. Apartment building property managers should board or replace windows, repair broken door jambs, change locks and keys, repair broken lights, trim bushes blocking views, and deploy a wide range of CPTED strategies.
- **Improve physical security.** Doing so enhances natural surveillance, visibility, sightlines, and access control. It also reduces piggybacking, trespassing, and other unauthorized access.
- **Block easy access to targets.** This can be done by installing doors, gates, screens, and other real or symbolic barriers to make the targets more difficult to access and any valuables more difficult to remove. Cash registers, vending machines, service vehicles, ATMs, and other high-value items may need to be moved. In stores, high-value items should be placed in locked glass cases. In gas stations, clerks should be behind break- and bullet-resistant polycarbonate.
- **Protect especially vulnerable targets.** Some targets cannot be moved, but removable bollards, roll-down gates, fences, and screens can deny access to them after hours.
- **Regulate access to high-risk assets or areas.** It may be necessary to require identification cards, permits, or fees for access to areas like bathrooms, parks, schools, and parking garages.

Capable Guardian

Routine activity theory suggests that the presence of capable guardians may deter crime. Criminals generally avoid targets or victims who are perceived to be armed, capable of resistance, or potentially dangerous. Criminals generally stay away from areas they feel are aggressively patrolled by police, security officers, or nosy neighbors. Likewise, they avoid passive barriers such as alarm systems, fences, locks, or related physical barriers.

Criminals look for the easiest, least-risky path. The concepts of natural surveillance and capable guardians can help reduce a site's perceived vulnerability and make it less attractive to offenders.

Situational Crime Prevention

Situational crime prevention was developed in the late 1970s and early 1980s in Great Britain. Although influenced by CPTED and defensible space concepts, situational crime prevention sought to reduce crime opportunities in all behavioral contexts, not just in buildings and other spaces.

Early situational crime prevention consisted of opportunity-reducing measures directed at specific forms of crime—for example, removing or deflecting potential offenders from target areas. Recent forms of situational crime prevention include strategies to reduce crime motives and opportunities, such as boundary-setting rules and stimulating the conscience of potential offenders. Such social prevention strategies link situational crime prevention to the emerging field of second generation CPTED. In short, situational crime prevention manages, designs, or manipulates the environment in a systematic way as permanently as possible—to increase the effort and risks of crime and reduce the rewards as perceived by a wide range of offenders.

British research caused crime control policy to shift its attention from offenders (and their personalities, behaviors, or backgrounds) to the environment (namely, factors that contribute to criminal behavior by creating opportunities for crime). Clarke (1983) contributed by developing crime prevention techniques that can be applied to almost any situation. Security practitioners can readily apply the techniques to their facilities. As Sorensen et al. note (1998):

Situational crime prevention is the crime prevention approach that utilizes rational choice theory as its theoretical framework, follows a methodology that analyzes the opportunities for a specific crime to occur in a particular situation, and prescribes solutions to remove those criminal opportunities.

Rational choice theory draws on the model of the likely offender who weighs the costs, risks, and rewards of committing a specific crime at a particular time and place. Situational crime prevention measures are effective because they are a practical, cost-effective and permanent alteration to the physical environment [and] are tailored to fit specific types of crime. Four overarching approaches that guide . . . situational crime prevention techniques are increasing the effort [needed to commit crime], increasing risks [associated with crime], reducing rewards [of crime] and removing excuses [for illegal behavior by inducing shame or guilt].

The four approaches to situational crime prevention are often accomplished as follows:

- Increasing the effort:
 - target-hardening measures, which increase the effort by creating physical barriers, such as locks, screens, steel doors, fences, and shatterproof glass
 - access control measures, which increase the effort by limiting access to vulnerable areas

- removal or deflection of offenders
- control of crime facilitators, which limits access to the tools criminals use to commit crimes (e.g., removing access to cans of spray paint, installing collect-call-only public telephones, removing shopping carts, towing abandoned cars, and screening for weapons)
- Increasing the risks:
 - entry and exit screening, which increases risk by monitoring who and what enters or exits an area
 - formal and mechanical surveillance with CCTV systems
 - surveillance by employees, concierges, parking attendants, and security officers
 - natural surveillance, which is bolstered with appropriate window placement, external lighting, limiting of blind spots, trimmed hedges, and pruned tree canopies
- Reducing anticipated rewards:
 - target removal, such as a no-cash policy, direct deposit of checks, and temporary removal of car radios
 - labeling of valuable property, which makes it more difficult for criminals to sell
 - reducing temptation by, for example, using gender neutral telephone listings and rapidly repairing vandalism and graffiti
 - denying the criminal his or her gain through, for example, plantings on walls vulnerable to graffiti, ink explosion kits in bank money bags, and personal identification numbers (PINs) for credit cards and car radios
- Removing excuses:
 - rule and boundary setting, which removes the ambiguity that allows people to commit offenses and excuse their crimes with claims of ignorance or misunderstanding
 - stimulating the conscience, often through declarations against shoplifting, speeding, smoking, drug use, littering, etc.
 - controlling disinhibitors, for example, through drug-free zones, weapon-free policies, drinking age laws, V-chips (age filters) for video stations, and age restrictions to pornographic Web sites
 - facilitating compliance, that is, making it easier to act in desirable ways than in undesirable ways (e.g., providing legitimate trash sites to stop illegal dumping or convenient trash bins for litter disposal)

Defensible Space

Newman studied the relationship between particular design features and crime in public housing developments in New York. The four components of Newman's study were to

- define perceived zones of territorial influence,
- provide surveillance opportunities for residents and their guests,
- place residential structures (public areas and entries) close to safe areas, and
- design sites and buildings so their occupants are not perceived as stigmatized or vulnerable.

The sites and buildings that were perceived as most vulnerable and isolated shared the following characteristics:

- unassigned open spaces that were unprotected and uncared for, providing opportunities for residents and outsiders to engage in illegitimate activities
- unlimited, uncontrolled access to the site, as well as numerous escape routes
- lack of territoriality and boundary definition, discouraging residents from claiming space and taking control of the site and preventing them from differentiating strangers from legitimate users
- a lack of natural surveillance and supervision
- design conflicts, placing incompatible activities next to each other

Using his theory of defensible space, Newman modified housing developments by implementing elements of CPTED design: high fences; designated paths; and architectural treatment to distinguish private, semi-private, semi-public, and public spaces. Defensible space design should link territoriality and surveillance by creating designs that lead people to consider the area as being within their sphere of influence, a place where they have a responsibility to prevent crime. People who live, work, and play in an area tend to feel a sense of ownership and responsibility and therefore try to protect the area.

Subsequent CPTED demonstration projects attempted to extend the defensible space concept to school, commercial, and transportation environments. They met with little success, as territorial behavior is much less natural there than in the residential context. In the late 1980s, Newman applied defensible space to the Five Oaks neighborhood in Dayton, Ohio. Controlling access to the neighborhood and reducing traffic restricted drug dealers' access to patrons in the area. Newman also attempted, with mixed success, to employ high levels of community involvement, extra police attention, and home ownership programs (Newman, 1996).

Newman's later work, emphasizing neighborhood self-help, echoes the writing decades earlier by Jacobs about community development, both social and physical, as the necessary ingredients for safe communities. It also launched efforts to expand CPTED into the realm where social prevention and opportunity reduction are balanced together—a new field called second generation CPTED.

Crowe and CPTED

Crowe (1991) refined Newman's ideas through his experience in the Westinghouse CPTED projects, establishing a CPTED taxonomy matching methods to the function of the crime area. He notes (1991) that

in the CPTED approach, a design is proper if it recognizes the designated use of the space; defines the crime problem incidental to and the solution compatible with the designated use; and incorporates the crime prevention strategies that enhance (or at least do not impair) the effective use of the space.

This came to be known as the 3-D approach (for definition, designation, and design). Under his leadership in the mid-1980s, the National Crime Prevention Institute taught CPTED to thousands of police officers.

Second Generation CPTED

Gregory Saville and Gerard Cleveland (2008) developed second generation CPTED to return physical CPTED to its origins in community development as outlined by Jacobs in *The Death and Life of Great American Cities* (1961) and Newman in *Communities of Interest* (1980). Those works emphasized not only reducing physical opportunities for crime but also creating a sense of neighborliness to help reduce motives that cause crime in the first place. Second generation CPTED can help security professionals identify social resources within the community that can enhance a crime prevention project.

In second generation CPTED, the legitimate activity supports employed in first generation CPTED are reinforced by developing community cohesion and a more permanent sense of neighborliness. Newman (1996, p. 48) observes that physical modifications

have made people realize they could intervene to change things, and . . . become active in city politics. . . . [R]einvestment in one's own property no longer has to be undertaken as a risky, individual act but as an activity done in concert with one's neighbors.

Second generation CPTED employs four main strategies (Saville & Cleveland, 2008):

- **Cohesion.** Techniques include community groups, neighborhood associations, and personal development programs (leadership training, financial, and organizational skills, conflict resolution, etc.).

- **Capacity threshold.** Also known as tipping point theory, this strategy balances land uses and urban features. For example, too many abandoned properties can tip an area into crime whereas a healthy balance of legitimate commercial properties, recreational facilities, and diverse residential properties can enhance livability
- **Community culture.** Cultural, artistic, sporting, and other recreational activities bring neighborhood people together in common purpose.
- **Connectivity.** Strategies link the neighborhood to surrounding neighborhoods and to funding and political support from corporations and upper levels of government.

CPTED 3-D and Beyond

The following is a tool for evaluating of the purpose or designation of a space, its definition in terms of management and identity, and its design as it relates to desired function and behavior management (sometimes referred to as the three Ds, but expanded here to include other aspects as well):

| Designation | Answers |
|------------------------------------------------------------------------------------------------|---------|
| What is the designated purpose of the space? | |
| For what purpose was it originally intended? | |
| How well does the space support its current or intended use? | |
| Is there a conflict? If so, how and where? | |
| Definition | |
| How is the space defined? | |
| Is the ownership of the space clear? | |
| Where are the borders of the space? | |
| Do any social or cultural definitions affect how the space is or may be used? | |
| Are legal and administrative rules clearly established in the policy and effectively enforced? | |
| Do signs indicate the proper use of the space or define the limits of access? | |
| Are there any conflicts or confusion between purpose and definition of the space? | |
| Design | |
| How well does the physical design support the intended function? | |
| How well does the physical design support the desired or accepted behaviors? | |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------|--|
| Does the physical design conflict with or impede the productive use of the space or proper functioning of the intended human activity? | |
| Is there any confusion or conflict in the way in which physical design is intended to control or modify behaviors? | |
| Deterrence | |
| Does the presence of security personnel deter illegitimate activity and promote intended behavior? | |
| Does the physical design and layout permit good surveillance and control of access to and from the property? | |
| Does the presence of intended behavior deter or discourage illegal or illegitimate activities? | |
| Detection | |
| Can one control entry to the property or building? | |
| Is there a process for assessing whether an intrusion is legitimate or illegitimate? | |
| Is intrusion detection accomplished by the physical design, mechanical technology systems, or operational manpower? | |
| After an intrusion, is a responding person or agency notified? | |
| Delay | |
| Are there passive barriers? | |
| Are there active barriers? | |
| Are there security officers or other designated responders? | |
| How much delay is needed to detect and respond? | |
| Response | |
| What are the roles and the post orders of the responding security officers? | |
| What equipment is needed to support a complete response? | |
| What tactics are used to respond quickly and clearly? | |
| What training is given to respond appropriately to the threat? | |
| Reporting | |
| What communications network is used for documenting intrusions or calling for assistance? | |
| What is the written protocol for incident reports? | |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| How is the documentation organized and stored? | |
| Is the information sufficiently detailed and clear? | |
| Discrimination | |
| Are staff trained to distinguish legitimate from illegitimate users or threats? | |
| Is the equipment sufficiently sensitive to distinguish false from real threats? | |
| Neutralization | |
| Has the threat been sufficiently deterred? | |
| Has the system been reset and tested to prevent complacency or false alarms? | |
| Have the criminals, attackers, or threats been controlled, law enforcement contacted, and the scene re-secured? | |
| In the event of fire, smoke, or flood, has the threat been neutralized and damage assessed, and the scene secured to prevent contamination or pilferage? | |

Once the questions have been answered, the space is assessed according to how well it supports natural access control, natural surveillance, and territoriality. The questions are intended to ensure there are no conflicts between the intended space, its activities, and expected behaviors. For example, if an access control system is difficult to use or experiences frequent outages, employees may prop doors open to make their routine travel more convenient. Such a case suggests that security designers and property managers chose a poor system and also failed to educate users on its operation.

3.2 REDUCING CRIME THROUGH ARCHITECTURAL DESIGN

By working with appropriate community and professional groups, security practitioners can integrate CPTED features into the facility design to reduce opportunities for crime. Integrating CPTED during initial planning is more cost-effective than making changes after construction has begun.

3.2.1 BUILDING PLANNING AND DESIGN

Designing without security in mind can lead to lawsuits, injuries, expensive retrofitting, and the need for additional security personnel. Security measures added after construction may distort important building functions, add to security personnel costs, and result in exposed, unsightly installations.

Architectural Planning Process

A building must meet specific functional criteria, from which the design evolves. The building should permit efficient job performance, meet the needs of the users, and protect the users from safety hazards and criminal acts.

The following steps illustrate a traditional building planning process:

- **Programming.** The owner informs the architect about the building's purpose and occupants.
- **Schematic design.** The architect processes the programming information and develops bubble diagrams reflecting circulation patterns and proximity relationships. The diagrams evolve into drawings of the floor plan, site plan, and elevations as the beginnings of engineering considerations.
- **Design development.** The architect presents ideas to the client and makes design corrections. The drawings become more sophisticated and include more engineering considerations, such as structural, mechanical, electrical, ventilation, and site planning issues. Drawings are put into a larger scale (typically 1/4 inch to 1 foot in the United States).
- **Construction documents or working drawings.** These are the final drawings prepared for construction purposes. All technical data are presented in the drawings and are accompanied by technically written specifications.
- **Bids for construction and selection of contractor.** The architectural drawings and specifications are put out to bid.

Security needs should be addressed in the programming phase of design. It is primarily the owner's or client's responsibility to define the potential threats to people, information, and

property and to determine the necessary level of security and the available budget. Owners, clients, and developers may need to consult a security professional to develop appropriate security strategies.

Security design poses three challenges for architects:

- **Determining requirements.** The design team should analyze the designated purpose of the space or building, examining the cultural, legal, and physical definitions of the prescribed, desired, and acceptable behaviors. The space can then be designed to support desired behaviors and the intended function of the space. The design team should inquire about existing policies and practices and integrate that information into the programming process.
- **Knowing the technology.** Rapid advances in security technology make it challenging to keep up-to-date. Many projects today involve security system specialists as part of the team. Still, architects need a basic understanding of security principles and must be able to evaluate and work with technical security specialists and security equipment manufacturers.
- **Understanding architectural implications.** Designs must integrate the complicated and sometimes conflicting goals of security and life-safety issues as well as other project variables and requirements. Space, function, and people must be planned to support the security objectives of detection, delay, and response to unwanted or criminal situations.

The architect then converts the security requirements into an architectural program. Like a restaurant menu, the program defines what will be produced and what it will cost. Architects generally make the basic design decisions about circulation, access, building materials, fenestration, and other features that can support or thwart overall security aims. From this point forward, security considerations require changes in drawings and specifications—and additional time and money.

In addition, many jurisdictions require security review by the police as part of the building-permit approval process. Inspectors evaluate the plans for obvious spots where assaults, muggings, break-ins, and other crimes of opportunity may occur. Many jurisdictions have security ordinances that require certain lighting levels and security doors and windows. Some corporations have policies requiring similar security reviews. If security is treated as one of the many design requirements, then the implementation and costs for such measures will be no more burdensome than fire safety features or landscaping requirements.

CPTED requires a different design approach than traditional target hardening, which focuses on barriers like locks, alarms, fences, and gates. That approach tends to overlook opportunities for natural access control and surveillance, but sometimes the natural and

normal uses of the environment can accomplish the effects of mechanical hardening and surveillance. Each of CPTED's three basic strategies—natural access control, natural surveillance, and natural territorial reinforcement—can be implemented through organized methods (staffing), mechanical methods (technology products), and natural methods (site planning, design, landscaping, and signage).

A checklist can be a useful tool for identifying ways to incorporate CPTED design principles into proposed projects. A sample checklist can be found in the appendix.

Access Control, Surveillance, and Territorial Reinforcement

Access control should be strongly considered in these areas:

- all entrances and exits to the site and building
- internal access points in restricted or controlled areas
- environmental and building features used to gain access (avenues of approach, trees, ledges, skylights, balconies, windows, tunnels)
- security screening devices (officer stations, surveillance, identification equipment)

The focus of access control strategies is to deny access to a crime target and create in offenders a perception of risk as well as detection, delay, and response. An organized method of access control is the use of security officers. Mechanical methods include target hardening with locks, card key systems, windows with protective glazing, special door and window hardware, and reinforced walls, floors, or doors. Natural methods include the use of spatial definition and circulation patterns, sometimes through security zoning.

Surveillance strengthens access control. Organized surveillance methods include police and security officer patrols. Mechanical methods include lighting and video, while natural strategies include windows, low landscaping, and raised entrances.

Site Development and Security Zoning

Whenever possible, security planning should begin during site selection. The goal is to find a site that meets architectural requirements and provides security advantages. The security analysis should assess conditions on-site and off-site, taking into account topography, vegetation, adjacent land uses, circulation patterns, neighborhood crime patterns, police patrol patterns, sight lines, areas for concealment, location of utilities, and existing and proposed lighting. Other key factors are access points and circulation patterns for vehicles, employees, service personnel, visitors, and off-site pedestrians.

The site analysis represents the first level of security defense planning, which considers the site perimeter and grounds. Site design measures can include walls, heavy plantings, fences, berms, ditches, lighting, and natural topographic separations. The following are questions to ask at this stage:

- What is the physical makeup of the site and how does it influence security?
- What are the land uses surrounding the site?
- What types of criminal activity take place in the area? How often?

A site with high security risks may not be automatically disqualified. The owner may choose the site but acknowledge the security threats and address them through design, technology, manpower, and security management.

There are many means for securing grounds against trespassing. The most common tools are walls, chain link fences, moats, and other barriers. Landscaping, too, can help, in part by establishing a property line that discourages unwelcome parties from entering the site.

The second level of security defense planning is the perimeter or exterior of the building. After the site perimeter and grounds, the building shell and its openings represent the crucial second line of defense against intrusion. The area being protected should be thought of as having four sides as well as a top and bottom. The principal points of entry are the windows, doors, skylights, storm sewers, roof, floor, and fire escapes.

Doors and windows inherently provide poor resistance to penetration. Attention must be paid to the doorframe, latches, locks, hinges, panic hardware and surrounding wall. Secure design of windows must consider the type of glazing material, the window frame, the window hardware, and the size of the opening.

The building shell itself is a security consideration, for the type of construction affects the level of security. Most stud walls and metal deck roof assemblies can be compromised with hand tools in less than two minutes. Unreinforced concrete block walls can be broken quickly with a sledgehammer or a car.

The third level of security for which the architect should design is internal space protection. Sensitive areas within a facility may warrant special protection with security technology, staffing, and restricted circulation. The level of protection may be based on zones of differing security levels. The idea is to allow employees, visitors, vendors, and others to reach their destinations and to prevent them from entering areas where they have no business. Controlling access to each department of a building, where appropriate, screens out undesirable visitors, reduces congestion, and helps employees identify and challenge unauthorized persons.

The following are several types of security zones:

- **Unrestricted zones.** Some areas of a facility should be completely unrestricted to persons entering during the hours of designated use. The design of unrestricted zones should encourage persons to conduct their business and leave the facility without entering controlled or restricted zones. Unrestricted zones might include lobbies, reception areas, snack bars, certain personnel and administrative offices, and public meeting rooms.
- **Controlled zones.** In these zones, a person must have a valid purpose for entry. Once admitted, the person may travel from one department to another without severe restriction. Controlled zones might include administrative offices, staff dining rooms, security offices, office working areas, and loading docks.
- **Restricted zones.** These are sensitive areas limited to staff assigned to those areas. Sections within restricted zones may require additional access control. Functions and departments located in restricted zones may include vaults, sensitive records, chemicals and drugs, food preparation, mechanical areas, telephone equipment, electrical equipment, control rooms, laboratories, laundry, sterile supply, special equipment, and sensitive work areas.

Once circulation patterns are successfully resolved through security zoning, mechanical solutions can be considered.

Visibility: Privacy Versus Security

Striking the right balance between privacy and security can be difficult. A low hedge or fence psychologically and physically says what is public property and what is private. A picket fence establishes an edge without obscuring the view or limiting surveillance. Adding trees may provide a sense of enclosure but still give the ability to see into the property between the fence and the tree canopy.

Block or brick walls may secure the property but also hide thieves. Bare walls invite graffiti. Walls supplemented with landscaping (such as thorny bougainvillea, carissa, or wild lime) can provide protection and a more effective barrier. Certain plants can also discourage trespassers even without a wall. Thorny shrubs could be a safety problem if small children are around, and such plants may pose a maintenance challenge. Many thorny plants come in different sizes to fit different landscaping needs. For example, carissa comes in three sizes: emerald blanket, which is a dwarf variety; boxwood blanket, which grows up to 6 feet (1.8 m); and carissa grandiflora, which grows to 7 or 8 feet (2.1 to 2.4 m).

In a residential application, hedges, shrub masses, or low ground coverage may discourage breaking and entering through windows. It is best to avoid tall, large-leaved plants that could

visually protect the intruder. Pygmy date palms in front of windows allow breezes through, but the needle-sharp thorns at the base of the palm fronds will slow down anyone climbing through them. Other plants that provide similar coverage are the Jerusalem thorn and cinnecord. Even if a burglar enters through a door and leaves through a window, it is much more difficult to carry out large stolen goods through bushes, hedges, ferns, and other landscaping barriers.

Earth berms are commonly used in landscaping and can be very effective in terms of natural access control. However, caution is warranted in some applications to ensure that they do not create visual obstructions. For example, a public park used berms to break up the monotony of the flat site, but the berms blocked police from viewing play areas used by local gangs. The berms had to be lowered to no more than 2.5 feet (0.7 m).

Landscaping can be an effective crime prevention measure, or it can create criminal opportunities. The following landscaping and planting considerations are critical for safe design:

- Plantings should not obscure extensive parts of a main path or recreation area.
- Plants' growth rates and maintenance requirements must be considered.
- Low-growing plants should be set back 1 yard (1 m) from the edge of paths or walkways.
- Low-growing shrubs should be kept no higher than 32 inches (81 cm) in height.
- Spiny or thorny shrubs should be used in potential hiding places or areas of illegitimate activity or along walls containing windows from which people should be kept away. Thorny plantings may attract litter; a low perimeter fence may be needed to keep windblown debris away.
- Hard landscaping should be vandal-resistant and not provide potential missiles, such as cobblestones or loose gravel.
- Landscape features and furniture should not provide a means to gain access to the property or to see over walls or hedges into rooms and gardens. Furniture should be designed for short-term use; it should not be usable for sleeping.
- Tree canopies should be trimmed up to 8 feet (2.4 m) in height where appropriate to provide a clear line of site and reduce hiding spots and ambush opportunities.

The type and placement of trees can drastically affect the coverage of exterior security lighting. Lighting for security should be from the tops of trees downward. A security professional should be involved in the landscaping and lighting plans. It is important to determine whether the trees are deciduous and shed their leaves or whether they remain full all year, like pine trees.

Tree type and placement also affects video surveillance. On a site plan, camera placement may seem to provide clear lines of vision. However, trees may cause blind spots. Both the height and fullness of the trees must be considered for camera placement.

3.2.2 OFFICE BUILDINGS

Office building construction (whether renovation, an addition, or new construction) may require security professionals and building owners to work with design professionals in new and challenging ways. An architect or other design professional needs information to develop the architectural program and design a secure building. The source of that information is typically the security director. If the client company has no security professional of its own, one may need to be contracted to provide the necessary knowledge and assistance to the company and architect.

The security professional should identify the corporate assets that are vital to protect. The three asset categories are people, information, and property.

Asset to Be Protected: People

Of course, people are the most valuable asset to be protected. In creating a needs assessment for the architect, the security professional should develop answers to the following questions:

- Who are the users? (visitors, staff, service crew, sales)
- What can the users do in the building? (tasks, recreation, work)
- Why are the particular users there? (official business, visiting as guests)
- When do the users arrive and leave? (shifts or other patterns)
- Where can users go in the building? (horizontal, vertical)
- How can the users get there? (access methods, circulation)

The security professional should prepare a table like the following for the architect:

| Who | Why | What | When | Where | How |
|----------------|-----------------------|----------------------------|------------------|------------------------|----------------------------------------------|
| Vice president | company business | administration; management | 8 am–6 pm M–F | all areas total access | staff elevator |
| Janitor | clean offices; vacuum | clean; collect trash | 1 am–4 am M–F | lobby floors | officer lets in, has keys to special service |

Taking the example of the janitorial role, the security implications might be as follows:

- control of after-hours access
- verification of cleaning employee status
- security staffing to sign in and supervise entry and exit
- key control

These security concerns could then translate into design implications, such as these:

- a sign-in desk for the service trades
- access control system to allow staff to control entry and log movements
- placement of garbage bins
- location of service elevator
- location of service doors
- alarm systems for offices and critical cabling to and from control room
- infrastructure lines and structure

The preceding is only a small sample of the issues and concerns that the architect must address based on information from the security professional.

The architectural program or problem-seeking stage should incorporate the information developed from answering the six questions. Later the information is used to develop schematic drawings, development drawings, and construction documents.

Asset to Be Protected: Information

The following are the critical questions to ask during the needs assessment:

- Who has access to the information? (staff, management, contractors/consultants, vendors, joint venture partners, mailroom) Also, who will have access to the facility after normal duty hours?
- What is the information? (data, trade secrets, personnel records, blueprints, computer programs, classified government information, third party information, operational or business plans)
- What format does the information reside in? (personal knowledge, hardcopy, electronic media, models/prototypes, equipment)
- How transportable and transferable is the information?
- Why is the information worth protecting? (competitive advantage, critical technology, strategic business value, regulatory requirements, privacy protections, contractual/legal restrictions)

- When is the information accessible or vulnerable (and for how long)?
- Where is the information accessible or vulnerable?
- How can the information legitimately and illegitimately be acquired or compromised?

After answering those questions, the security professional should prepare an information protection plan for the architect.

With this information it is possible to develop architectural, technological, and organizational responses that support a comprehensive information asset protection strategy.

Architectural design changes could do the following to address the security professional's concern for information protection:

- **Doors and windows.** Minimize the number of exterior penetrations, and make them easily observable. Doors can be controlled and monitored for accountability. The main entrance can be architecturally defined. The service entrance can be secured and supervised. Storage rooms can be monitored and placed where a supervisor can oversee movement. Consider the visibility of information, activities and equipment through windows (internal and external).
- **Reception desk.** Design a reception desk or counter that screens visitors, vendors, and other outsiders. The counter or reception desk should be designed to view all entry doors and elevators if provided. The reception area establishes the layering of public versus private entry into the building. The design should be such that computer screens, visitor logs, and other security-related information are not visible to visitors or non-authorized personnel.
- **Controlled areas.** Clearly distinguish and restrict access as appropriate to controlled areas including VIP areas, computer/data center facilities and areas where sensitive operations occur.
- **Computer room.** Design the computer room for strict access control, protected utility lines, and high-security glazing for easy supervision, and place it in a central location.
- **Computer anchoring.** Secure computers with anchor pads.
- **Employee traffic patterns.** Control employee ingress and egress. Controlled, supervised egress makes it possible to screen packages, briefcases, and purses. Staff locker areas should be well-lighted and supervised to prevent theft.
- **Elevators.** Design elevators to open into the supervised core area. Special floors or VIP offices may require elevator access control or dedicated elevators.
- **Loading dock.** Establish a separate road to the loading dock, away from employee or visitor travel. The loading dock should be designed with ground loops and an intercom

to notify security staff when a truck is in the loading area during hours when personnel are not directly supervising it. When possible, shipping and receiving areas of the loading dock should be physically separated.

- **Mail room.** Locate the mail room at the end of a clear, unobstructed line of travel from the loading or mail delivery area. The mail room should be a secure room with monitoring of the door to provide controlled access and accountability.
- **Vaults.** Place vaults, fire safes, and record files appropriately for the site and the frequency of use. For example, supermarkets place vaults in the front of the store for visibility, while other stores hide their vaults.
- **Conference/meeting facilities.** Establish a conference center or suite of meeting rooms outside the restricted area of an office building or plant (usually off the main lobby, but before the security access control point. This prevents the need to “badge in” visitors who are attending meetings or events while also keeping them outside the restricted (private or semi-private) areas of the building.

Asset to Be Protected: Property

In examining property, the same process (asking the six questions and determining security and architectural criteria) applies. Companies that carefully work through the process can gain a real market advantage by designing out shoplifting, pilferage, espionage, assaults, and terrorism.

A building may present many environmental conflicts that provide opportunities for offenders. CPTED and defensible space principles can help planners and architects prevent or reduce those opportunities.

Building owners may not have control over various environmental factors, such as the neighborhood streets; nearby stadiums, bars, parks, or waste dumps; or public services, including police protection. However, if the security professional properly assesses the risks and develops a needs assessment for the architect, the correct solutions will emerge.

CPTED for Offices and Office Buildings

Offices and office buildings are vulnerable to walk-in thefts, burglary, theft by deception and fraud, vandalism, loss of information, and employee theft. After identifying the crime risks, the security professional should consider various design requirements for site security, building security, and internal security:

- **Site location.** Study the zoning and building code restrictions for the site and surrounding area. Examine existing and proposed landscaping.
- **External areas.** Carefully design garages and parking lots. Arrange entrances, exits,

paths, and roads to minimize circulation conflicts and security issues. Identify and prioritize fences, gates, and site lighting. Design video surveillance after circulation patterns are laid out. Pay attention to delivery and waste disposal areas.

- **Access points.** Design access points for employees, visitors, and service personnel. Limit the number of building entrances. If needed, use additional exit-only doors. Consider fire exits and life safety code requirements early so as to not undermine security. Identify loading bays and design them for secure shipping and receiving. Note the security needs of basement areas and mechanical rooms. Consider the arrangement of external stairways, roof access, doors, and windows.
- **Internal locations.** Carefully design and arrange lobby entrances, secondary entrances, reception areas, cash office areas, computer areas, electrical or telephone service areas, executive areas, canteens, staff restrooms, security command centers, vault rooms, and special equipment.
- **Lobby entrance.** Design the lobby entrance to establish to all that the lobby is the correct place to enter. Use higher-grade materials in the lobby to create an image of success, stability, and power.
- **Reception desk.** Design the lobby reception desk to serve as a layer in building security. Consider directing the receptionist to identify and approve visitors before allowing them further into the building. Position the reception desk to provide a good view of persons entering the building and perhaps to block access to nonpublic areas, elevators, and stairs. Do not overload the receptionist with an excessive number of duties that would distract from the screening function. Install an emergency assistance call button. If appropriate, design the desk to conceal any video surveillance equipment and to accommodate viewing angles and ventilation requirements. Also, design the desk in a way that slows attacks (as bank teller counters are built wide to prevent criminals from easily reaching or jumping over them).
- **Access control and video surveillance.** Attend to these issues during building design and architectural programming. Examine stairs, elevators, and corridors for security requirements. Select a key system that can accommodate growth and change.
- **Pedestrian access.** Design a path that leads directly from the street to the front of the building.
- **Orientation.** Orient the building to allow views into the site.
- **Doors and windows.** Pay extra attention to these, especially on the ground floor.
- **Conduits.** Plan for conduits that can serve security needs. Lay out conduit paths (with sufficient capacity for future needs) during building design to avoid expensive renovations later. Consider whether any lines should be shielded to protect communications.

3.2.3 **INDUSTRIAL BUILDINGS**

Industrial buildings are subject to a high risk of employee theft, burglary, robbery, commercial espionage, vandalism, and arson. Using CPTED principles, industrial buildings can be designed to reduce the opportunities for such crimes. Listed below are several steps the architect or security professional can take to implement CPTED principles in an industrial setting:

- **Traffic.** Clearly define incoming and outgoing traffic.
- **Perimeter.** Clearly define the perimeter boundaries with landscaping, fences, walls, etc.
- **Paths of travel.** Separate the paths used by public, private, and service vehicles and pedestrians. Provide pedestrian access routes and points that are easily viewed by others.
- **Building shell.** Minimize openings in the building shell. Lobbies and entrances should be clearly defined and provide a transition from the security perimeter to the plant or production area. Reinforce or otherwise secure any openings in the building shell that are larger than 96 square inches (619 square cm) and lower than 18 feet (5.5 m) from the ground. Options include polycarbonate glazing, window laminates, screens, and other devices. If a perimeter door must be left open for ventilation, add a chain link door to permit air flow and visibility while maintaining security.
- **Monitoring.** Arrange for exterior doors used as emergency exits to be alarmed, placed under video surveillance, and monitored by security staff.
- **Service doors.** Arrange service doors from the outside to lead directly to service areas to minimize interior pedestrian traffic. Service doors should be under in-person or video surveillance.
- **Shipping and receiving.** Separate the two functions as much as possible to minimize collusion and pilferage opportunities. The dock area should be inside the building to minimize the exposure of materials. It should also provide a driver waiting area with restrooms to minimize traffic through the building.
- **Trash.** Design the trash removal system so custodial staff can access compactors or incinerators without leaving the building.
- **Research and development.** Place research and development and other business-sensitive activities away from the building's normal circulation paths.
- **Employee entrances.** Place them directly off any employee parking lots. Design doorways to be large enough to accommodate the traffic flow and to permit supervision by staff for pilferage control.
- **Punch clocks.** Place these near the employee entrance, separated by barriers for controlled ingress and screening of IDs by security staff.

- **Personnel office.** Place this near the outer edge of the building to minimize applicants' travel through the building.
- **Elevators.** Separate freight and personnel elevators to reduce the exposure of freight to theft and pilferage.
- **Warehouse.** Place finished product warehousing areas away from operational areas. Establish access control for doors to warehousing areas.
- **Other storage.** Design tool rooms and other storage areas to have a ceiling enclosure.

3.2.4 **PARKING FACILITIES**

Parking lots and garages can use CPTED features to increase environmental security with surveillance, access control, and territorial reinforcement. The interface of design, security patrol, and technology provides the means to achieve these CPTED goals.

Vulnerability Assessment

The first step toward CPTED-based parking lot security is the vulnerability assessment. Generally, in the United States, the standard of care dictates that the assessment include a criminal history of the site; a review of landscaping, lighting, stairwells, elevators, surveillance capabilities, access control equipment, signage, and restrooms; and an inspection of any facilities for supervision or revenue collection. The policies and procedures for the operation and staffing of the parking facility should also be scrutinized.

As in other settings, the security professional should ask the who, why, what, when, where, and how questions, such as the following:

- Who does the parking facility serve—shoppers, commuters, students, or employees?
- How many cars frequent the facility, and how quickly do spaces turn over?
- Are the lines of sight clear, or are they blocked by walls, columns, or ramps?
- What are the hours of operation, and how do those hours affect the user environment?
- Is the lighting all or mostly natural, or is it mostly artificial? Are lighting fixtures at ceiling height? If so, what is the color of the ceiling and how are the lights placed?
- Is video surveillance in use? If so, what are the details of the system?
- Does the garage or lot have ground-level protection, such as gates, screens, or other barriers?

Additional questions might address vehicle and pedestrian entrances, required paths for handicap accessibility, elevator condition, stairwell placement and visibility issues, and whether lightly used areas can be closed selectively.

Among the threats commonly associated with parking facilities are thefts of vehicles; thefts from vehicles; attacks against persons, such as assault, robbery, and rape; and vandalism.

On the Ground

To maximize natural surveillance, it is best to place a surface parking lot where it can be viewed from the road and nearby occupied buildings.

Perimeter definition and access control can deter unwanted pedestrian access to a garage or lot. It can take the form of fencing, level changes, ground-floor protection, and other architectural and environmental barriers that channel people to designated entry points and discourage others from hiding outside or inside the facility.

Ground-level metal screening should be used to deter unauthorized access, while upper floors should be open-sided but have cable strung to prevent cars from overshooting the parking spaces. Screened, rather than walled, ground levels and open upper levels allow natural surveillance and make it more likely that calls for assistance will be heard. Ground-level screening should not be floor to ceiling, however, as it can give a criminal a way to climb to higher floors. Short bushes close to the perimeter wall may discourage persons from climbing or cutting the screen. Exterior doors to the garage should allow egress only.

Additional landscaping should be varied in size. Instead of planting a solid hedge, it is more effective to combine low hedges and high-canopy trees. All trees and bushes must be properly maintained to provide a good field of vision and to avoid creating hiding places. Plantings that are higher than 3 feet (1 m) should not be placed within 10 to 15 feet (3 to 4.5 m) of entrances to prevent hiding spots. Mature trees should be trimmed of low branches to a height of 8 feet (2.5 m).

Traffic engineers prefer multiple access points to increase circulation patterns. However, with more entrances it is more difficult to control the users and uses of the facility. CPTED theory prefers one means of entry and exit for all vehicles at the parking facility. If the traffic volume requires more, each access point should have an attendant booth, access gate arm, roll down shutter for after-hours closure, video surveillance, and good lighting.

Pedestrian access is often overlooked or poorly designed at parking facilities. A primary rule is to avoid forcing pedestrians to cross the paths of the cars whenever possible. When such encounters are unavoidable, the design should create a safe passage for persons to move along until they come to a marked crosswalk that cautions drivers to take notice. Architects

can design the pedestrian paths to intersect with or pass by the parking attendant station to create an opportunity for surveillance. Handicap accessibility may require dedicated parking spaces and special attention to ramps, railings, floor surfaces, pedestrian crossovers and paths, stair design, and elevator location and design.

Garage booth attendants may be both guardians and crime victims. For example, in 2006 at the City Place Mall in West Palm Beach, Florida, a parking attendant observed two men loitering suspiciously in the parking garage. She locked herself in the booth, but she did not have a radio or telephone to call for assistance. The robbers broke in with a baseball bat, beat the attendant, and took the contents of her cash drawer.

Booths should be situated with a 360-degree field of view, be monitored by a video surveillance system, and possess security glazing, duress alarms, and drop safes with signage advertising that the attendant cannot retrieve money. The booths must also have adequate lighting to support video surveillance. Lighting should be dimmable to allow the attendant to see outside at night. The attendant's restroom should be located near the booth in an area open to surveillance opportunities. The restroom should be locked and have a personal alarm inside in case of attack.

CPTED-minded designers should exclude public restrooms from their designs as they are a natural meeting place for victims and predators and are difficult to secure because of privacy issues. If the inclusion of public restrooms is unavoidable, they should be placed so that the doors are visible from the attendant's normal working position. The bathrooms should have open maze-type entrances that allow cries for assistance to be heard. Panic and assistance call stations and motion-activated lighting should also be installed.

Automatic pay stations should be placed where they are visible to users and staff to reduce the opportunity for vandalism, burglary, or attacks on customers.

Structural Elements

If a facility is being newly built, round columns should be used as they allow for greater visibility than rectangular or square columns. Also, the most CPTED-oriented ramp design is an exterior loop that allows floors to be level and preserves unobstructed lines of sight. Where solid walls are needed, portholes with screening, windows, or openings should be incorporated to create an openness that encourages and enables casual observance.

Stairwells and elevators should be located centrally and should be visible from the attendant's position. If such placement is impossible, video surveillance should be installed to monitor comings and goings. Panic alarms and door position switches should be installed to alert the booth attendant that someone is in a stairwell.

Stairwells should be visible from grade level and be constructed of clear glazing materials to allow visibility from the street. Stairwell terminations at the lowest level should not offer accessible hiding holes, and exits onto the roof, if it not also a parking level, should be secured to prevent unauthorized access. Doors to mechanical rooms on the roof level should always be locked. Both basement and rooftop doors should be wired for door-position switches, intercoms, screech alarms, and signal transmission to security or police.

Elevators, like stairwells, should incorporate as much glass and high-visibility placement as structurally possible. Glass-walled elevators placed along the exterior of the building provide for good natural visibility by persons on the street and within the garage. They should have intercom capability and audible alarms.

The stairs and elevators of high-rise or subsurface parking garages that serve offices, residences, or other mixed uses should have elevators that empty into a lobby, not directly to business or residential floors. Persons exiting at the lobby must then use another bank of elevators or stairs that can be subject to screening, access control, and surveillance by security staff, if desired.

Surveillance

Video surveillance cameras should be placed in areas with constant light, whether daylight or luminaires (lamps). Low-light cameras can be used, but they are more expensive and they represent a tacit admission that lighting conditions might be poor.

Cameras should be placed to achieve an unhindered view. On surface parking lots, cameras should have good lines of sight and cover as much ground as possible. The cameras should be protected within dark polycarbonate domes to resist vandalism and to obscure where the cameras are watching.

Video surveillance systems in parking facilities should be monitored in real time and digitally recorded for playback and enhancement. Color cameras make it easier to identify specific vehicles and persons, a useful capability for evidence.

Panic button call boxes should be integrated with the video surveillance system, allowing a camera to be activated when a call box is pushed. Video surveillance systems can also be integrated into the access control system so that license plate numbers are captured when vehicles enter or exit the facility.

Lighting

Without good lighting, video surveillance systems and natural surveillance are impaired. Lighting in garages is addressed in detail in Guideline on Security Lighting for People, Property, and Public Spaces (Illuminating Engineering Society of North America, 2005). It

recommends lighting levels of 5 to 6 foot-candles (54 to 65 lumens per square meter) in gathering areas such as stairs, elevators, and ramps. Walkways around garages should have 5 foot-candles of lighting. Open parking lots should have a minimum of 3 foot-candles (32 lumens per square meter), as should open parking lots in retail shopping areas and parking lots for hotels, motels, and apartment buildings. Entrances should have 10 foot-candles (108 lumens per square foot) of lighting or twice the level of lighting in the surrounding area to make them stand out and increase visibility. Perimeter fencing should have at least half the average horizontal illumination on both sides of the fence to reduce hiding spots.

The height of the light fixtures makes a difference in the ability of pedestrians to see past the shadows caused by cars and other obstructions. Typical light poles are 30 to 45 feet (9 to 14 m) high and cast a wide swath of lighting, but they create deep shadows between cars. Pedestrian-level lighting that is about 12 to 14 feet (3.6 to 4.2 m) high casts light that will go through the glass of cars and reflect off the cars, reducing shadows and dark spots. Pathways to garages should be lit to 3 foot-candles (32 lumens per square meter) to allow visibility of persons at least 30 feet (9 m) away, with an average-to-minimum lighting ratio not to exceed 4:1. Ideally, an open parking lot should have a combination of high and low lighting to maximize coverage and visibility and minimize shadows and hiding opportunities.

The interior of parking garages should be painted in light colors to increase light reflection. Luminaires should use polycarbonate lenses to resist vandalism and other breakage. A maintenance protocol should be established to ensure that damaged lights are repaired and burned-out bulbs replaced promptly, and working bulbs should be replaced on a schedule based on their life expectancy.

One innovative measure taken by a garage in Fort Lauderdale, Florida, was to paint the ceiling in white circles that reflected the light from the luminaires. The ceilings of this garage were higher than most, allowing better light distribution.

Different light sources produce different qualities of light. Most CPTED practitioners prefer metal halide lamps because they last about 20,000 hours and accurately reproduce the color of cars, clothes, and people. Low-pressure sodium vapor lamps typically last about 50,000 hours and are the most energy-efficient, but their poor color rendition makes them unsatisfactory for capturing crime scene details. High-pressure sodium vapor lamps and mercury vapor lamps are less expensive than metal halide lamps but do not last as long and do not render colors as well. There is no one right answer for all facilities. The CPTED approach allows for diversity in lighting, based on the risk and threat assessment and the desired user experience.

Signage

Parking facility signage should be well lit, with letters or symbols that are at least 8 inches (20 cm) tall. Wall signage for pedestrian and vehicular traffic should be graphic whenever possible to ensure universal understanding and provide a clear sense of direction.

Graffiti in parking environments is a form of illegitimate signage, which often represents a designation of turf by gangs or vandals. It should be removed as quickly as possible. The CPTED-minded architect can also take steps to discourage graffiti. For example, wall surfaces can be coated with graffiti-resistant epoxy paint, and lighting levels can be increased in problem areas to increase the potential for natural surveillance. Attempts to prevent graffiti tell vandals that the property is the territory of its rightful owners.

Mixed Uses

The territoriality of desired site users is being increased by a new trend: making parking part of a mixed-use development. By having legitimate users in and around the parking facility more often, the garage increases the number of legitimate users and casual eyes on the street.

Many garages are adding retail storefronts, such as copying facilities, fast food eateries, or car washes to provide compatible, safe activities that draw legitimate users. Additionally, parking may be reserved during the day for businesses, but at night the lot may offer flat-fee parking for area nightclubs, restaurants, and nearby residents with overnight permits.

3.2.5 SCHOOLS

Schools—with their large populations, multiple entrances, and many ground floor windows—present a protection challenge. Problems may arise when the following conditions are present:

- Campus borders are poorly defined.
- Informal gathering areas are out of sight.
- The building layout produces isolated spots.
- Bus loading conflicts with car traffic.
- Student parking lots are farthest from the building.
- Street parking by students creates conflict with the neighborhood.
- Parking areas are obscured by plantings.
- Locker areas create confusion and facilitate the hiding of contraband.
- The overuse of corridors creates blind spots.
- Restrooms are located away from supervision.

Clearly, school security is much affected by school design. CPTED can contribute to a school's security through natural access control, surveillance, territoriality, boundary definition, management, and maintenance. Moreover, CPTED can make those contributions without turning the school into a fortress. Security technology can often complement CPTED measures.

A security professional applying CPTED principles to school design should focus on the following areas and systems:

- **Site:** landscaping, exterior pedestrian routes, vehicular routes and parking, and recreational areas
- **Building design:** building organization, exterior covered corridors, points of entry, enclosed exterior spaces, ancillary buildings, walls, windows, doors, roofs, and lighting
- **Interior spaces:** lobby and reception areas, corridors, toilets and bathrooms, stairs and stairwells, cafeterias, auditoriums, gyms, libraries and media centers, classrooms, locker rooms labs, shops, music rooms, computer rooms, and administrative areas
- **Systems and equipment:** alarms and surveillance systems, fire control, HVAC (heating, ventilating, and air conditioning) and mechanical equipment, vending machines, water fountains, elevators, telephone systems, and information systems

A school's relationship with its immediate surroundings is communicated through its edges. Landscaping can be used to denote school boundaries and, if desired, restrict access. Territoriality and defined use can also be expressed through perimeter fencing and gates, which should be constructed to allow a view for natural surveillance. Although plantings can improve the aesthetics of these barriers, the planting arrangement must not be allowed to create hiding places.

Administrative offices should have clear views of the play, gathering, and parking areas. Perpetrators will be discouraged from trespassing and illegal behavior because of the increased risk of identification and intervention. Legitimate users will feel safer. Design features should also allow views into and out of courtyards, classrooms, and high-risk areas.

Numerous other issues arise in CPTED-oriented school design:

- **Observation from classrooms.** Parking and circulation areas should be placed in view of the classrooms. The high volume of students in classes means a greater chance for casual observation.
- **Observation of vehicular traffic.** Administrative spaces should have clear lines of sight to entry roads and parking lots. No one entering a school area should go undetected.
- **Surveillance points.** Providing views to potential problem areas from publicly used

spaces, such as a common-use stairwell, ensures that many people will be observing at any given time.

- **Exterior circulation.** Paths should be large enough to accommodate many students. Students should be prevented from using exterior paths as informal gathering places. Bicycle racks should be placed in a high-visibility area.
- **Traffic calming.** To prevent speeding, parking lots should be designed with few or no long runs. Proper speed and stop signage must be installed and maintained. Bus pickup/ drop-off areas should not conflict with other traffic.
- **Signage.** Signage should announce intended and prohibited uses. Signage should be clear, reasonably sized, and placed for easy viewing.
- **Spatial/temporal issues.** It can be useful to place safe activities in unsafe locations—for instance, having hallways near offices for natural surveillance and supervision or using the school after hours for adult education. Separating the cafeteria entrance and exit by space can help define movement and prevent conflicts. Temporal separation, too, can help—for example, scheduling different lunch times for older and younger students. Conducting driver education in school parking lots increases supervision in otherwise high-risk areas.
- **Lighting.** It is helpful to have dusk-to-dawn lighting on the grounds.
- **Covered circulation.** Blind spots and entrapment points must be minimized. Potential “door in the face” incidents must be eliminated.
- **Main entry.** Main entryways should be obvious and few in number. Access to other areas from main entryways should be carefully planned and not obscured. The potential for getting confused and lost should be limited. Weapon detectors can be integrated within an entryway.
- **Recessed entries.** Blind spots should be avoided. When building configuration creates a blind spot, it helps to taper corners to allow students to see around the corner and avoid an ambush.
- **Doors and doorways.** Recessed doorways can create dangerous blind spots if designed poorly. Doors and frames must be institutional grade to withstand heavy use and abuse. Faceplates should be used over locks to prevent jimmying.
- **Courtyards and other gathering places.** Formal gathering places should be well-defined, well-lighted, and under observation. If basketball, volleyball, or tennis courts are attracting nuisance behavior after hours, the nets and hoops can be removed at the end of each day. If the gym is used after hours, it is important to be able to lock off the rest of the building or campus.
- **Walls.** Walls should not be allowed to create hiding places. Walls located in high vandalism areas should be constructed of durable material resistant to graffiti and

vandalism. Landscaping may be able to provide a buffer against walls that are susceptible to graffiti.

- **Windows.** A group of small windows can provide the same benefits as a large window but with greater security, as the smaller size makes it difficult to crawl through or get property out. Clerestory windows along the top of a wall provide light and ventilation without allowing easy entry. A glass-block wall with clerestory windows minimizes wall penetrations and provides both security and natural lighting. All windows should feature self-engaging locking mechanisms.
- **Video surveillance.** Cameras should operate continuously, and recordings should be archived.
- **Duress alarms.** These should be placed in isolated areas like restrooms and locker areas. The alarms should be integrated with the overall security system.
- **Computers.** As valuable items, computers should be individually secured and regularly checked.

3.2.6 **AUTOMATED TELLER MACHINES**

Automated teller machines (ATMs) are where the easy money is.² Criminals know ATMs are often located in isolated locations and that users are likely to be withdrawing cash or making a deposit. Implementation of CPTED principles can reduce the risk of assault, robbery, and murder of bank customers. The following are some key considerations:

- **Ensure adequate lighting at and around ATMs.** Adequate lighting allows users to see any suspicious people near the ATM and allows potential witnesses, including police, to see a crime in progress and view the offender. Sufficient lighting should be in place around all building corners adjacent to the ATM, as well as for nearby parking places. Lighting should illuminate the ATM itself and surrounding areas to prevent hiding places and shadows.

The United States has no national guidelines or standards for bank facility lighting. However, some cities and states have such standards. Standards' typical lighting minimums at and around ATMs are 25 foot-candles (269 lumens per square meter) at the face of the ATM, 10 foot-candles (107 lumens per square meter) within 5 feet (1.5 m) of the face of the ATM, and 2 foot-candles (22 lumens per square meter) 50 to 60 feet (15 to 18 m) away from the ATM, measured at 3 feet (1 m) above the ground.

² This section is adapted from Scott (2001) and Atlas (2008).

According to lighting designers, however, most minimum lighting standards do not address all the factors that affect visibility. Shadows, light types, light colors, light direction, light uniformity, glare, and obstructions all affect visibility. When light is very bright at the face of the ATM and very low in the surrounding areas, users may not be able to see approaching dangers or persons in hiding.

Lights should turn on automatically with photo sensors. Once set, lighting levels should be monitored regularly to ensure they do not fall below acceptable levels. Long-lasting light bulbs should be used. Automated light-detection monitors can alert the ATM operator if light levels drop. In addition, light fixtures must be protected so offenders cannot disable them.

- **Ensure that landscaping around ATMs allows for good visibility.** Trees and shrubbery should be trimmed routinely to remove potential hiding places for offenders and ensure the ATM is visible to passers-by. Slow-growing shrubbery is preferable. Obstacles such as trash bins, benches, or walls that obstruct views of the ATM should be removed.
- **Install mirrors on ATMs.** Rearview mirrors on ATMs and adjacent building corners may enable ATM users to detect suspicious people and behavior.
- **Install ATMs where natural surveillance is plentiful.** ATMs should be placed in locations that provide natural surveillance from pedestrians and drivers and that lie within the view of police patrols and surveillance cameras. Opportunistic criminals typically avoid open, unobstructed locations because crime there is more likely to be observed and reported to police or private security. Moreover, natural surveillance increases the probability of assistance to the victim when a robbery occurs. When ATMs are placed in enclosures or vestibules, there should be large vision panels, free of obstructions, to allow customers to conduct transactions without being ambushed. Vestibules should have duress alarms that summon a real response. People who service ATMs are also vulnerable to robbery and should be considered in the security design (e.g., by having duress alarms and secure closets to service the machines).

ATMs are increasingly being placed inside businesses, such as grocery and convenience stores, with much natural surveillance. Indoor ATMs should be free of sight obstructions like plants and blinds and should be visible from the street.

The ATM itself is sometimes a target. It may require alarm system components, shock and seismic sensors, sufficient weight and tensile strength, heat detectors, and locking mechanisms to deter attacks against the machine itself.

- **Install ATMs in police stations.** Some jurisdictions have installed publicly accessible ATMs in police stations for safety. Stations that cannot accommodate the added vehicle and pedestrian traffic could limit ATM use to nighttime hours when the risk of robbery is greatest and level of other activity at the station is lower. ATMs can also be installed in or near other government buildings, such as post offices or fire stations, where natural surveillance may be available.
- **Use extra precautions at high-risk sites.** ATM operators should examine local crime rates when assessing the risk level at potential ATM sites. ATMs should not be placed in areas known for drug trafficking or near abandoned property or crime-prone liquor establishments. In areas with particularly high crime rates, it may be necessary to move, close, or limit the hours of ATMs.
- **Use surveillance cameras.** Surveillance cameras around ATMs serve two main purposes: deterring robbery and fraud and identifying offenders. Cameras should record both close-up images of the ATM user and the view immediately behind the user.

Plainly visible cameras are more effective deterrents to robbers but are more vulnerable to vandalism. Dummy surveillance cameras should not be used unless there are also working cameras at the site—otherwise, the dummy cameras could create a false sense of security among ATM users and lead to a security negligence lawsuit (on grounds called “illusion of security”). At least one ATM operator has installed heat sensors around the ATM that detect the presence of people out of view of surveillance cameras. The sensors can activate either a recorded voice message warning the person to move away from the ATM or a silent alarm.

- **Install devices to allow victims to summon police during a robbery.** Examples include the following:
 - Panic button. However, panic buttons may lead to a false-alarm problem.
 - Telephone next to the ATM.
 - Live microphone in the ATM. A security company can monitor it and respond if needed.
 - Door alarm. An alarm can be set to activate if a door to an enclosed vestibule is left open too long.
 - Reverse PIN (personal identification number) technology. An ATM user can activate a silent alarm by entering his or her PIN in reverse order or by entering an additional digit after the PIN. However, such a system may be cost-prohibitive and hard for victims to use when they are under stress.

- **Deploy private security officers.** Security officers can be assigned to high-risk ATMs only or can randomly patrol many ATMs. This is an expensive measure.
- **Prohibit loitering and panhandling near ATMs.** Some robbers loiter around ATMs, waiting for a suitable victim; in other cases, aggressive panhandlers try to obtain money from ATM users. Laws that prohibit loitering and panhandling near ATMs give police the authority to keep opportunistic offenders away from potential victims.
- **Require that ATMs be located in enclosed vestibules with doors that lock.** Such a requirement may help, but it could also result in a customer being trapped in the vestibule with an offender. Moreover, ATM users habitually open or hold doors for others, and such vestibules tend to attract homeless people.
- **Set daily cash-withdrawal limits.** Such limits could reduce the potential financial loss from a robbery and discourage robbers who decide that the benefits of the robbery are not worth the risk of apprehension. However, most street robbers do not expect much cash from a robbery and are willing to take the risk. (Many drug-crazed robbers will kill for \$20.)
- **Train users.** Customers should be taught to
 - put money away discreetly before they leave,
 - look around to see if they are being observed,
 - take a companion when they visit an ATM at night,
 - look inside the vestibule before entering,
 - prevent persons in line from looking over the customer's shoulder to observe the PIN, and
 - watch the parking area for loiterers and keep an eye out for hiding places, such as trash bins and parked cars.

3.2.7 **U.S. FEDERAL BUILDINGS**

The bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995 led to a federal effort to develop security standards for all federal facilities. Several U.S. state governments have also established standards for their buildings.

The General Services Administration (GSA) security standards encourage a defensible space/CPTED approach. Edges and boundaries of the properties should clearly define the desired circulation patterns and movements. Various techniques should be used to screen legitimate users from illegitimate users who might look for opportunities to commit crimes.

The GSA security standards address security glazing, bomb-resistant design and construction, landscaping and planting designs, site lighting, and natural and mechanical surveillance opportunities. Different recommendations apply to different security levels. For example, a Level 1 facility might not require an entry control system while a Level 4 facility might require electronic controls and video surveillance.

The standards call on architects and engineers to implement security measures in four different categories:

- Perimeter and exterior security
 - parking area and parking controls
 - video surveillance monitoring
 - lighting with emergency backup
 - physical barriers
- Entry security
 - intrusion detection system
 - upgrade to current life safety standards
 - mail, person, and package screening
 - entry control with video surveillance and electric door strikes
 - high-security locks
- Interior security
 - employee IDs and visitor controls
 - control of access to utilities
 - emergency power for critical systems
 - location of day care centers
- Security planning
 - locations of tenants based on their particular security needs
 - blast standards

The criteria balance cost-effectiveness, acceptance of some risk, and the need for federal buildings to be accessible to the public.

Given the risk of bombing at federal buildings, security professionals and architects should consider taking the following defensive steps to prevent such attacks or minimize their effect:

- Establish a secure perimeter around the building, as far out as possible. Setbacks of 100 ft. (30 m) are suggested.

- Design concrete barriers as flower planters or works of art and position them near curbing at a distance from the building with less than 4 ft. (1.2 m) of spacing between them to block vehicular passage.
- Build new buildings in a simple rectangular layout to minimize the diffraction effect when blast waves bounce off U-shaped or L-shaped buildings.
- Reduce or eliminate building ornamentation that could break away in a blast, causing further damage to building occupants or pedestrians. External cladding should be lightweight to minimize damage if it goes flying due to a bomb or severe weather.
- Eliminate potential hiding places near the facility.
- Provide unobstructed views around the facility site, and place the facility within view of other occupied facilities.
- Eliminate lines of vehicular approach perpendicular to the building.
- Minimize the number of vehicle access points.
- Eliminate or strictly control parking beneath facilities.
- Locate parking as far from the building as practical, and place it within view of occupied rooms or facilities.
- Illuminate the building exterior.
- Secure access to power or heat plants, gas mains, water supplies, and electrical and telephone service.

In the coming years, street crime and workplace violence will continue as major threats, and they may be joined by sabotage and terrorism against critical infrastructure. CPTED may not be able to stop the most determined terrorists or other criminals, but even acts of terrorism usually start with trespassing and unauthorized access as the property is scoped for vulnerabilities. A criminal or terrorist may seek a different or more vulnerable target if the original target is not easily accessible or has a proper security system in place. Therefore, CPTED is a legitimate strategy for reducing the opportunity for acts of terrorism as well as more common criminal acts.

APPENDIX A

CPTED SAMPLE SURVEY

This checklist helps the user incorporate CPTED design principles into proposed projects. It was adapted from a list developed by the Federal Way (Washington) Department of Community Development Services (City of Federal Way, 2009).

Please fill out the checklist to indicate which strategies have been used to implement CPTED principles in your proposed project. Please check all strategies that are applicable to your project for each of the numbered guidelines. You may check more than one strategy for each guideline.

1. NATURAL SURVEILLANCE

1.1 Blind corners. Avoid blind corners in pathways and parking lots.

- Pathways should be direct. All barriers along pathways should be permeable (see through) including landscaping, fencing etc.
- Consider the installation of mirrors to allow users to see ahead of them and around corners.
- Other strategy used: _____

1.2 Site and building layout. Allow natural observation from the street to the venue, from the venue to the street, and between uses.

For Non-Single Family Development

- Orient the main entrance toward the street or both streets on corners.
- Position habitable rooms with windows at the front of the dwelling. Access to dwellings or other uses above commercial/ retail development should not be from the rear of the building.
- Offset windows, doorways, and balconies to allow for natural observation while protecting privacy.

For Commercial/ Retail/ Industrial and Community Facilities

- Locate main entrances/exits at the front of the site and in view of the street.
- If employee entrances must be separated from the main entrance, they should maximize opportunities for natural surveillance from the street.
- In industrial developments, administration/offices should be located at the front of the building.

For Surface Parking and Parking Structures

- Avoid large expanses of parking. Where large expanses of parking are proposed, provide surveillance such as security cameras.
- Access to elevators, stairwells, and pedestrian pathways should be clearly visible from an adjacent parking area.
- Avoid hidden recesses.
- Locate parking areas in locations that can be observed by adjoining users.

For Common/Open Space Areas

- Open spaces shall be clearly designated and situated at locations that are easily observed by people. Parks, plazas, common areas, and playgrounds should be placed in the front of buildings. Shopping centers and other similar uses should face streets.
- Other strategy used: _____

1.3 Common/open space areas and public on-site open space. Provide natural surveillance for common/open space areas.

- Position active uses or habitable rooms with windows adjacent to main common/open space areas, e.g. playgrounds, swimming pools, etc., and public on-site open space.
- Design and locate trash bin enclosures in a manner which screens refuse containers but avoids providing opportunities to hide.
- Locate waiting areas and external entries to elevators/stairwells close to areas of active uses to make them visible from the building entry.
- Locate seating in areas of active uses.
- Other strategy used: _____

1.4 Entrances. Provide entries that are clearly visible.

- Design entrances to allow users to see into them before entering.
- Entrances should be clearly identified.
- Other strategy used: _____

1.5 Fencing. Fence design should maximize natural surveillance from the street to the building and from the building to the street, and minimize opportunities for intruders to hide.

- Front fences should be predominantly open in design, e.g. pickets or wrought iron, or low in height.
- Design high, solid-front fences in a manner that incorporates open elements to allow visibility above the height of 5 feet.

- If noise insulation is required, install double glazing at the front of the building rather than solid fences higher than five feet.
- Other strategy used: _____

1.6 Landscaping. Avoid landscaping that obstructs natural surveillance and allows intruders to hide.

- Trees with dense, low-growth foliage should be spaced, or their crown should be raised to avoid a continuous barrier.
- Use low groundcover, shrubs a maximum of 32 inches (0.8 m) in height, or high-canopied trees (clean trimmed to a height of 8 feet or 2.4m) around children's play areas, parking areas, and along pedestrian pathways.
- Avoid vegetation that conceals the building entrance from the street.
- Other strategy used: _____

1.7 Exterior lighting. Provide exterior lighting that enhances natural surveillance. For specific security lighting requirements, refer to the Guideline on Security Lighting for People, Property, and Public Spaces (Illuminating Engineering Society of North America, 2005).

- Prepare a lighting plan in accordance with Illuminating Engineering Society of North America standards, which address project lighting in a comprehensive manner. Select a lighting approach that is consistent with local conditions and crime problems.
- Locate elevated light fixtures (poles, light standards, etc.) in a coordinated manner that provides the desired coverage. The useful ground coverage of an elevated light fixture is roughly twice its height.
- For areas intended to be used at night, ensure that lighting supports visibility. Where lighting is placed at a lower height to support visibility for pedestrians, ensure that it is vandal-resistant.
- Ensure that inset or modulated spaces on a building facade, access/egress routes, and signage are well lit.
- In areas used by pedestrians, ensure that lighting shines on pedestrian pathways and possible entrapment spaces.
- Place lighting to take into account vegetation, in its current and mature form, as well as any other element that may have the potential for blocking light.
- Avoid lighting of areas not intended for nighttime use to avoid giving a false impression of use or safety. If danger spots are usually vacant at night, avoid lighting them and close them off to pedestrians.
- Select and light "safe routes" so that these become the focus of legitimate pedestrian activity after dark.

- Prevent climbing opportunities by locating light standards and electrical equipment away from walls or low buildings.
- Use photoelectric rather than time switches for exterior lighting.
- In projects that will be used primarily by older people (retirement homes, congregate care facilities, senior and/ or community centers, etc.), provide higher levels of brightness in public/common areas.
- Other strategy used: _____

1.8 Mix of uses. In mixed-use buildings, increase opportunities for natural surveillance while protecting privacy.

- Where allowed by city code, locate shops and businesses on lower floors and residences on upper floors. In this way, residents can observe the businesses after hours while the residences can be observed by the businesses during business hours.
- Include food kiosks, restaurants, etc. within parks and parking structures.
- Other strategy used: _____

1.9 Security bars, shutters, and doors. When used and permitted by building and fire codes, security bars, shutters, and doors should allow observation of the street and be consistent with the architectural style of the building.

- Security bars and security doors should be visually permeable (see-through).
- Other strategy used: _____

2. ACCESS CONTROL

2.1 Building identification. Ensure buildings are clearly identified by street number to prevent unintended access and to assist persons trying to find the building.

- Street numbers should be plainly visible and legible from the street fronting the property.
- In residential uses, each individual unit should be clearly numbered. In multiple-building complexes, each building entry should clearly state the unit numbers accessed from that entry. In addition, unit numbers should be provided on each level or floor.
- Street numbers should be made of durable materials, preferably reflective or luminous, and unobstructed (e.g. by foliage).
- For larger projects, provide location maps (fixed plaque format) and directional signage at public entry points and along internal public routes of travel.
- Other strategy used: _____

2.2 Entrances. Avoid confusion in locating building entrances.

- Entrances should be easily recognizable through design features and directional signage.
- Minimize the number of entry points.
- Other strategy used: _____

2.3 Landscaping. Use vegetation as barriers to deter unauthorized access.

- Consider using thorny plants as an effective barrier.
- Other strategy used: _____

2.4 Landscaping location. Avoid placement of vegetation that would enable access to a building or to neighboring buildings.

- Avoid placement of large trees, garages, utility structures, fences, and gutters next to second-story windows or balconies that could provide a means of access.
- Other strategy used: _____

2.5 Security. Reduce opportunities for unauthorized access.

- Consider the use of security hardware and/or human measures to reduce opportunities for unauthorized access.
- Other strategy used: _____

2.6 Signage. Ensure that signage is clearly visible, easy to read, and simple to understand.

- Use strong colors, standard symbols, and simple graphics for informational signs.
- Other strategy used: _____

For Surface Parking and Parking Structures

- At the parking entrance, provide pedestrians and drivers with clear directions to stairs, elevators, and exits.
- In multi-level parking areas, use creative signage to distinguish between floors to enable users to locate their cars easily.
- Advise users of available security measures (such as security phones or an intercom system) and where to find them.
- Provide signage in the parking area advising users to lock their cars.
- Where exits are closed after hours, ensure this information is indicated at the parking area entrance.
- Other strategy used: _____

3. OWNERSHIP

3.1 Maintenance. Create a “cared for” image.

- Ensure that landscaping is well maintained to give an impression of ownership, care, and security.
- Where possible, design multi-unit residential uses such that no more than six to eight units share a common building entrance.
- Other strategy used: _____

3.2 Materials. Use materials that reduce the opportunity for vandalism.

- Consider using wear-resistant laminate, impervious-glazed ceramics, treated masonry products, stainless steel materials, anti-graffiti paints, and clear oversprays to reduce opportunities for vandalism. Avoid flat or porous finishes in areas where graffiti is likely to be a problem.
- Where large walls are unavoidable, consider the use of vegetative screens.
- Furniture in common areas or on the street should be made of long-wearing, vandal-resistant materials and secured by sturdy anchor points, or it should be removed after hours.
- Other strategy used: _____

REFERENCES

- Agnew, R. (1995). Determinism, indeterminism, and crime: An empirical exploration. *Criminology*, 33, 83–109.
- ASIS International. (2007). *Information asset protection guideline*. Alexandria, VA: ASIS International.
- Atlas, R. (2008). *21st century security and CPTED*. Boca Raton, FL: Taylor & Francis Publisher.
- Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. In M. Tonry and N. Morris (Eds.), *Crime and justice: An annual review of research* (pp. 225–256). Chicago, IL: University of Chicago Press.
- Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588–608.
- Crowe, T. (1991). *Crime prevention through environmental design: Applications of architectural design and space management concepts*. Boston, MA: Butterworth-Heinemann.
- Erikson, R. (2003). *Teenage robbers and how and why they rob*. San Diego, CA: Athena Research Corporation.
- Illuminating Engineering Society of North America. (2005). *Guideline on security lighting for people, property, and public spaces*. New York, NY: Illuminating Engineering Society of North America.
- Jacobs, J. (1961). *The death and life of great American cities*. New York, NY: Vintage Books.
- Jeffery, C. R. (1971). *Crime prevention through environmental design*. Thousand Oaks, CA: Sage Publications, Inc.
- Newman, O. (1973). *Defensible space: Crime prevention through urban design*. New York: Macmillan.
- Newman, O. (1976.) *Design guidelines for creating defensible space*. Washington, DC: U.S. Government Printing Office.
- Newman, O. (1980). *Communities of interest*. New York: Springer Verlag.
- Newman, O. (1996). *Creating defensible space*. Washington, DC: U.S. Department of Housing and Urban Development.
- New Zealand Ministry of Justice. (2005). *National guidelines for CPTED in New Zealand: Part 1: Seven qualities of safe places*. Wellington, New Zealand: Ministry of Justice.
- Pezzin, L. (1995). Criminal careers. *Journal of Criminal Law and Criminology*, 11, 29–50.
- Scott, M. (2001). *Robbery at automated teller machines*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing.

Siegal, L. (1999). *Criminology* (6th ed.). Florence, KY: West Wadsworth Publishing Co.

Sorensen, S., Walsh, E. M., & Myhre, M. (1998). *Crime prevention through environmental design in public housing: Resource manual for situational crime prevention in public housing and community settings*. Bethesda, MD; SPARTA Consulting Corporation.

Taylor, R., & Harrell, A. (1996). *Physical environment and crime*. Washington, DC: National Institute of Justice.

Weisel, D. L. (2005). *Analyzing repeat victimization*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing.

Wilson, J. Q., & Kelling, G. (1982.) Broken windows. *Atlantic Monthly*, 211, 29–38.

PPS FUNCTION **DETECTION**

The physical protection systems function of detection is addressed in the next five chapters:

- Sensors
- Video Subsystems and Alarm Assessment
- Lighting
- Alarm Communication and Display
- Entry Control

CHAPTER 4

SENSORS

4.1 KEY SENSOR CONCEPTS

This chapter discusses the sensors found in security systems. Sensors are the basic building blocks of an intrusion detection system. They initiate the detection function of the security system, indicating an intrusion attempt or a tamper event. All logical discrimination, transmission, processing display, and recording activities that occur after the initial alarm are due to the technology on which the sensor is based, including optical, electronic, electro-mechanical, or mechanical capabilities. If the sensor is inappropriate for the operating environment or the threat, or is not installed, operated, maintained, and tested properly, the output of the entire system is severely limited, becoming a greater burden than benefit.

The National Burglar and Fire Alarm Association strives to reduce nuisance alarms to one a year for each system, so device selection is paramount. In reality, it is highly unlikely that an effective sensor would have such a low nuisance alarm rate. It is critical to properly match the sensor to the threat and operating environment and integrate it into the overall physical protection system (PPS).

Intrusion detection systems include exterior and interior intrusion sensors, video alarm assessment, entry control, and alarm communication systems working in combination. Intrusion detection is the process of detecting a person or vehicle attempting to gain unauthorized entry into an area. The intrusion detection boundary should be thought of as a sphere surrounding the protected item so that all intrusions, whether by surface, air, underwater, or underground, are detected. Exterior intrusion detection technology tends to emphasize detection on or slightly above the ground surface, though emphasis on airborne intrusion is increasing. This chapter primarily covers ground-level intrusion.

4.1.1 **PERFORMANCE CHARACTERISTICS**

Three main characteristics of intrusion sensor performance are probability of detection (PD), nuisance alarm rate, and vulnerability to defeat. Understanding these characteristics aids the design and operation of intrusion sensor systems. The characteristics apply to both exterior and interior sensors.

Probability of Detection

A perfect probability of detection would be 1. However, in real life a sensor's PD is always less than 1. After thousands of tests, a sensor's PD only approaches 1.

For any specific sensor and scenario, the two values PD and confidence level (CL) are used to describe the effectiveness of the sensor. Manufacturers often state values of PD without stating the CL. In such cases, they are likely implying a value of at least 90 percent for CL.

The probability of detection depends primarily on these factors:

- target to be detected (e.g., walking/running/crawling intruder, tunneling, etc.)
- sensor hardware design
- installation conditions
- sensitivity adjustment
- weather conditions
- condition of the equipment

Such conditions vary, so a specific PD cannot be assigned to each component or set of sensor hardware. Any PD assigned to a sensor is conditional, based on assumptions about conditions. An intrusion sensor may have one PD for a low-level threat, such as a vandal, and another, lower PD against a more sophisticated threat. The design basis threat drives system design. If the design basis threat consists of three criminals with substantial knowledge and skill, the site should employ a sensor with a higher PD, since the adversary is more capable. If the threat consists of teenage vandals, a lower PD can be tolerated. Sensor selection must match the application and environment.

The system designer should specify the detection criteria for a sensor or sensor system. This specification should note what will be detected, what actions are expected, any other considerations such as weight or speed of movement, and what probability of detection is required. An example of a detection criterion might be as follows:

The perimeter intrusion detection system shall be capable of detecting a person, weighing 35 kilograms or more, crossing the detection zone by walking, crawling, jumping, running, or rolling, at speeds between 0.15 and 5 meters per second, or climbing the fence at any point in the detection zone, with a detection probability of 90 percent at 95 percent confidence.

This represents a clear and measurable set of conditions, not just a statement such as “successful detection should occur most of the time.” When a high PD is required at all times and under all expected weather conditions, the use of multiple sensors is recommended. Contingency plans and procedures are needed so compensatory measures can be implemented in the event of loss of any or all sensors.

Nuisance Alarm Rate (NAR)

A nuisance alarm is any alarm not caused by an intrusion. The nuisance alarm rate states the number of nuisance alarms over a given period. In an ideal system, the nuisance alarm rate would be zero. However, all sensors interact with their environment, and they cannot always discriminate between adversary intrusions and other events. That is why alarm assessment is needed. It is not effective to send the security officer force to respond to every alarm. Alarm assessment determines the cause of the alarm and decides whether a response is needed. Without assessment, detection is incomplete.

Nuisance alarms have many causes. Natural causes include vegetation (trees and weeds), wildlife (animals and birds), and weather conditions (wind, rain, snow, fog, lightning). Industrial causes include ground vibration, debris moved by wind, and electromagnetic interference.

False alarms are nuisance alarms generated by the equipment itself (whether by poor design, inadequate maintenance, or component failure). Different types of intrusion sensors are more or less vulnerable to various nuisance or false alarm sources.

In designing a system, it is important to specify an acceptable false alarm rate (FAR). One could specify that the FAR for the total perimeter intrusion system shall not average more than one false alarm per week, per zone, while maintaining a PD of 0.9. This statement is much more meaningful than simply saying that a higher FAR and NAR may be tolerated if they do not result in system degradation (which is harder to measure). With specific values for false alarm rates, it is easier to decide whether to report a sensor to maintenance personnel.

Vulnerability to Defeat

An ideal sensor cannot be defeated; however, all existing sensors can be defeated. Different types of sensors and sensor models have different vulnerabilities to defeat. The objective of the PPS designer is to make the system very difficult to defeat. There are two general ways to defeat the system:

- **Bypass.** Because all intrusion sensors have a finite detection zone, any sensor can be defeated by going around its detection volume.
- **Spoof.** Spoofing is any technique that allows the target to pass through the sensor's normal detection zone without generating an alarm.

4.1.2 **ALARM INITIATION CONDITIONS**

Sensors of all types should be included in the PPS to initiate alarms under any of the following conditions:

- **Occurrence of a potential intrusion event.** These are intrusion sensors.
- **A change in a safety or process condition being monitored (rise in temperature, presence of smoke, etc.).** These are state sensors.
- **Loss of electrical power.** These are fault event sensors.
- **Opening, shorting, or grounding of the device circuitry or tampering with the sensor's enclosure or distributed control panels (transponders).** These are tamper sensors.
- **Failure of the sensor itself.** This is another fault event that should be detected.

4.1.3 **OPERATING CONDITIONS**

Units for indoor use should be capable of operating in a temperature range of 32° F to 120° F (0° C to 49° C). Units to be installed outdoors or in unheated structures should be capable of operating in temperatures ranging from -30° F to 150° F (-34° C to 66° C). All units should be capable of operating at 90° F (32° C) with 95 percent relative humidity.

4.2 **STANDARDS**

There are many manufacturers of the various types of sensors now available. It is important that users have standards against which to judge the quality and appropriateness of sensors. Several authoritative bodies provide guidance.

4.2.1 **UL STANDARDS**

Perhaps the best known of these is Underwriters Laboratories (UL), headquartered in Northbrook, IL. UL prepares safety standards primarily as a guide to device manufacturers, and then certifies whether devices submitted to the laboratories for approval meet those standards. The standards themselves are developed in response to broad feedback from the public, the insurance industry, government, academic bodies, inspection authorities, consumer organizations, and end users.

UL standards are publicly available, but UL urges the users of approved devices to be guided by the periodic UL directories instead of the standards. The directories are listings of specific

devices that have been submitted, tested, and certified by UL as meeting the requirements of a particular standard. (The directory that lists security devices is the *Automotive, Burglary Protection and Mechanical Equipment Directory*.) For asset protection professionals and other sophisticated users, however, a more detailed knowledge of the standard is important so that the full effect of a UL approval can be appreciated.

It often happens that UL approval is a requirement found in specifications for security systems and in municipal building and fire codes. UL standards are listed at www.ul.com. UL has promulgated numerous standards that apply to fire and security systems, mostly related to the engineering and manufacture of alarms and related controllers. It is important to emphasize that these are safety standards, not security standards, and thus provide guidance only as to the proper way to install devices so the danger of fire or other safety events is reduced. While safety is an important consideration when implementing a PPS, these standards do not address devices' vulnerabilities or their ability to detect intrusions by malevolent adversaries.

Of the following security system standards, those in bold type are especially relevant for security installers and users because they specify the manner of installation or operation:

Standard Numbers and Names

- 365 Police Station Connected Burglar Alarm Units and Systems
- 606 Linings and Screens for Use with Burglar Alarm Systems
- 609 Local Burglar Alarm Units and Systems
- 611 Central-Station Burglar Alarm Systems
- 634 Connectors and Switches for Use with Burglar Alarm Systems
- 636 Hold-Up Alarm Units and Systems
- 639 Intrusion Detection Units
- 681 Installation and Classification of Mercantile and Bank Burglar Alarm Systems**
- 1037 Anti-Theft Alarms and Devices
- 1076 Proprietary Burglar Alarm Units and Systems**
- 1610 Central Station Burglar Alarm Units
- 1635 Digital Burglar Alarm Communicator Units
- 1641 Installation and Classification of Residential Burglar Alarm Systems**

Each of these UL Standards has also been designated a national standard by the American National Standards Institute (ANSI).

4.2.2 **ASTM STANDARDS**

The American Society for Testing and Materials (ASTM), in Philadelphia, has established a committee to deal with security standards (Committee F-12, Security Systems and Equipment). The scope of the committee as defined by ASTM is

to develop and standardize nomenclature, definitions, test methods, specifications, classifications, and recommended practices for security systems and equipment and promotion of knowledge as it relates to security systems and equipment for security of property and safety of life. This work will be coordinated with other ASTM Technical Committees, organizations and individuals in this area.

ASTM standards have not yet been developed for security alarm systems or sensors. However, ASTM has published *Building Security* (Stroik, 1981), which is described as a “publication to establish a reference base for the evaluation and performance of building-related security systems, components and equipment.” One section of the text is devoted to devices and is titled “Design Considerations for High Security Interior Intrusion Detection Systems.”

4.2.3 **OTHER STANDARDS AND SPECIFICATIONS**

The U.S. General Services Administration (GSA) first published a specification for alarm system components in 1969. That specification, then known as Interim Specification WA-0045A, was twice revised, once in 1973 (Interim Spec. WA-0045B) and again in 1990. The latest revision, W-A-45OC/GEN, is a regular rather than interim document.

In 1976, a comprehensive report was issued by Sandia Laboratories, Albuquerque, NM, titled *Intrusion Detection System Handbook*. The material was prepared by members of the Sandia Laboratories staff, under the sponsorship of the former ERDA Division of Safeguards and Security (DSS). It was based on data obtained from evaluation programs, conducted at various laboratories, sponsored by DSS, the ERDA (now Department of Energy), Division of Military Application, the Department of Defense (DOD), and other governmental agencies, and on information provided by commercial security equipment suppliers. The original publication has undergone several revisions and is now released in the following volumes:

- Intrusion Detection System Concepts
- Considerations for Sensor Selection and Subsystem Design
- Exterior Intrusion Sensors
- Interior Intrusion Sensors
- Alarm Assessment Systems
- Alarm Reporting Systems
- Intrusion Detection System Integration

Although not intended to be used as specifications or standards for devices, the handbook covers various aspects of the use of intrusion detection devices in useful detail.

The National Fire Protection Association (NFPA) publishes detailed standards for municipal, central station, proprietary, and local fire alarm systems. Previously released as separate documents, NFPA Codes 71, 72A, 72B, 72C, 72D, 72E, 72F, 72G, 72H, and 74 were consolidated in 1993 into a single NFPA 72, National Fire Alarm Code. The association also publishes the National Fire Alarm Code Handbook, an explanatory text to assist in interpreting and applying the formal language of the code.

4.3 **EXTERIOR SENSORS**

4.3.1 **CLASSIFICATION**

There are several ways of classifying the many types of exterior intrusion sensors. In this discussion, five methods of classification are used:

- passive or active
- covert or visible
- line-of-sight or terrain following
- volumetric or line detection
- application

Passive or Active

Passive sensors operate in two manners. Some detect energy emitted by the object of interest, while others detect a target-caused change in a natural field of energy. Sensors that detect emitted energy include those that detect mechanical energy from a human walking on the soil or climbing on a fence. A sensor that detects changes in energy fields might, for example, monitor the local magnetic field caused by the presence of a metal. Both types of passive sensors use a receiver to collect energy emissions. The sensors may detect vibration, heat, sound, or capacitance.

Active sensors operate differently. They transmit energy and detect changes (caused by the presence or motion of a target) in the received energy. Active sensors typically contain both a transmitter and a receiver. Types of active sensors include microwave, infrared, and other radio frequency (RF) devices.

Passive and active sensors each have their strengths and weaknesses. Because a passive sensor does not emit energy, an adversary will have difficulty finding it, and the device is likely safer to use in environments containing explosive vapors or materials. Active sensors have the advantage of creating fewer nuisance alarms because of their stronger signals.

Covert or Visible

Covert (or hidden) sensors present certain advantages. Being hidden (for example, underground), they are more difficult for an intruder to detect, and they do not affect the appearance of the environment. By contrast, visible sensors (perhaps attached to a fence or structure), being detectable, may deter intruders from acting. Visible sensors are also usually easier to install, repair, and maintain.

Line-of-Sight or Terrain-Following

To work well, line-of-sight (LOS) sensors require a clear LOS in the detection space between the transmitter and receiver. To use such sensors where the terrain is not flat requires extensive site preparation.

A different type of sensor is the terrain-following sensor, which detects equally well on flat and irregular terrain. Transducer elements and a radiated field follow the terrain, creating uniform detection throughout the detection zone.

Volumetric or Line Detection

A volumetric sensor generates an alarm when an intruder enters the detection volume. It may be hard for an intruder to determine that a space is under detection.

Line detection sensors detect motion along a line. Some line detection sensors detect fence motion if an intruder moves the fence fabric where the sensor is attached. The detection zone of a line detection sensor is usually easy for an intruder to identify.

Application

Sensors can be grouped into various categories. Considering their mode of application in the physical detection space, one can divide sensors into these clusters:

- buried line
- fence-associated
- freestanding

Many sensor technology reviews have been published and supplement the material presented in this chapter (Barnard, 1988; Cumming, 1992; Fennelly, 1996; Williams, 1988).

4.3.2 **TYPES OF EXTERIOR INTRUSION SENSORS**

This section describes the most common exterior sensors at a very high level. Additional details can be found in Garcia (2006 and 2008). The use of exterior perimeter sensors is generally limited to government, nuclear, or correctional installations.

Ported Coaxial Cables

Ported coaxial cable sensors are active, covert, terrain-following sensors buried underground. Also called leaky coax or radiating cable sensors, they respond to the motion of material with a high dielectric constant or high conductivity. Human bodies and metal vehicles have those characteristics.

The outer conductor of this type of coaxial cable does not provide complete shielding for the center conductor, so some of the signal leaks through the ports of the outer conductor. The detection volume of ported coax sensors extends about 1.5 to 3.0 ft. (.46 m to .91 m) above the surface and about 3 to 6 ft. (.91 m to 1.83 m) wider than the cable separation. This type of sensor is more sensitive in frozen soil than in thawed. Some of the field energy is absorbed by conductive soil, and the conductivity of frozen ground is less than that of thawed ground.

Moving metal objects and moving water are both major potential sources of nuisance alarms by ported coaxial cable sensors. To avoid distorting the field, nearby metal objects or utility lines should be excluded from the detection volume.

The probability of detection (PD) of ported coaxial cable is affected by processor settings, orientation of the intruder, soil characteristics, and the presence of metal, including large amounts of salt or metals in the soil.

Fence Disturbance Sensors

Fence disturbance sensors are passive, visible, terrain-following sensors. They are usually installed on chain-link fences. They are considered terrain-following because the chain-link mesh itself follows the terrain.

These sensors can detect motion or shock, aiming primarily to detect an intruder who climbs on or cuts through the fence material. Several kinds of transducers are used to detect the fence's movement or vibration, such as switches, electromechanical transducers, strain sensitive cable, piezoelectric crystals, geophones, fiber-optic cable, and electric cable.

Nuisance alarms may be caused by wind, debris blown by wind, rain driven by wind, hail, and seismic activity from nearby traffic and machinery. The use of rigid fence posts and tight fence fabric minimizes nuisance alarms. Fence posts should move no more than 0.5 in. (12.7 mm) for a 50 lb. (22.7 kg) pull applied 5 ft. (1.5 m) above the ground. Fence fabric should

deflect a maximum of 2.5 in. (6.4 cm) for a 30 lb. (13.6 kg) pull centered between fence posts. Installing fence sensors on the inner fence of a two-fence system can reduce nuisance alarms by enabling the outer fence to block blowing trash or other debris and keep small animals away from the inner, sensed fence. It is best not to place movable objects on the fence (such as signs or loose ties), or nuisance alarms may result.

Ways to defeat a fence disturbance sensor include tunneling under the fence or crossing above the fence without touching it. To deter digging, one can place concrete under the fence and potentially even put the bottom edge of the fabric in the concrete. The PD of fence disturbance sensors depends not only on installation issues (fabric tension, fence processor settings, fence rigidity, noise coupled to the fence) but also on the adversary's approach to defeating the fence. If the adversary climbs over the fence using a ladder and never touches the fence, the PD will be very low or zero.

Sensor Fences

Sensor fences are passive, visible, terrain-following sensors that form the fence out of the transducer elements themselves. They are designed primarily to detect climbing on or cutting the fence. They are seen in various configurations.

Taut-wire sensor fences consist of many parallel, horizontal wires with high tensile strength, connected under tension to transducers. The transducers detect deflections of the wires, such as those caused by an intruder cutting the wires, climbing on the wires to get over the fence, or separating the wires to climb through the fence. The wire is typically barbed, and the transducers are mechanical switches, strain gauges, or piezoelectric elements. Taut-wire sensor fences can be mounted on existing fence posts or installed on an independent row of posts.

Sensor fences tend to be less susceptible to nuisance alarms than fence disturbance sensors because the transducers are not sensitive to vibrations and require a force of approximately 25 pounds on the wire to cause an alarm. However, sensor fences are vulnerable to the same defeat methods as fence disturbance sensors. For taut-wire fences, most nuisance alarms come from large animals walking into the fence, improper installation or maintenance, and ice storms.

The PD of taut-wire fences is affected by several factors: the tension of the wires, wire friction, and wire spacing. If the spacing between two wires is large enough to allow a person to pass through undetected, the PD will be much lower than if spacing is kept to 4 in. (10 cm) or less (Greer, VTW-250 and VTW-300, 1990).

Electric Field or Capacitance

Electric field or capacitance sensors are active, visible, terrain-following sensors designed to detect a change in capacitive coupling among a set of wires attached to, but electrically isolated from, a fence. The sensitivity of such sensors can be adjusted to extend up to 3.3 ft. (1 m) beyond the wire or plane of wires. However, high sensitivity typically leads to more nuisance alarms. Electric field and capacitance sensors may be triggered by lightning, rain, fence motion, and small animals. Ice storms may damage the wires and insulators. Good electrical grounding of the sensors and of metal objects in the sensor field can reduce nuisance alarms. Compared to other fence-associated sensors, electric field sensors are more difficult to defeat by digging under or bridging over because the detection volume extends beyond the fence plane (Follis, 1990).

These sensors can be mounted on their own posts instead of on a fence. When they are used without a fence, the absence of the chain-link mesh leads to a wider detection volume and a lower nuisance alarm rate. For freestanding applications, some electronic signal processing techniques employ additional wires in the horizontal plane to reduce the effects of distant lightning and small animals.

Freestanding Infrared Sensors

Infrared (IR) sensors used for exterior intrusion detection are active, visible, line-of-sight, freestanding sensors. In such systems, an IR beam is transmitted from an IR light-emitting diode through a collimating lens. At the other end of the detection zone, the beam is received by a collecting lens that focuses the energy onto a photodiode. If an opaque object blocks the beam, the IR sensor detects the reduction in received infrared energy. These sensors operate at a wavelength of about 0.9 microns, which is not visible to the human eye.

For high-level security applications, it is normal to use multiple-beam sensors, as a single IR beam is too easy to defeat. A multiple-beam IR sensor system usually includes two vertical arrays of IR transmitter and receiver modules. The number and configuration of modules depends on the manufacturer. The IR sensor creates an IR fence of multiple beams. Multiple-beam sensors usually incorporate electronics to detect attempts to spoof the beams with an alternative IR source.

Atmospheric conditions (fog, snow, dust storms) can block the IR beams and cause nuisance alarms. Grass, other vegetation, and animals may also cause nuisance alarms. The area between the IR posts should be kept clear since even trimmed grass may move in the wind and cause an alarm. Other sources of nuisance alarms include ground heave, optical misalignment, and deep snow.

The detection volume cross-section of a multiple-beam IR sensor is typically 2 in. (5 cm) wide and 6 ft. (1.8 m) high. Thus, like fence sensors, IR sensors have a narrow plane of

detection. IR beams travel in a straight line, so IR sensors are considered line-of-sight sensors and require a flat ground surface. A convex ground surface would block the beam, and a concave surface would allow an intruder to pass under the beam without detection. Digging under the bottom beam is possible unless there is a concrete sill or paved surface. The PD is very high for a multiple-beam sensor, but such sensors can be defeated through bridging, pole vaulting, or stepping or sliding through beams.

Bistatic Microwave Sensors

Bistatic microwave sensors are active, visible, line-of-sight, freestanding sensors. In a typical installation, two identical microwave antennas are installed at opposite ends of the detection zone. One is connected to a microwave transmitter operating near 10 Gigahertz (GHz) or 24 GHz. The other is connected to a receiver that detects the received microwave energy. The amount of energy received is equal to the vector sum of the direct beam between the antennas and the microwave signals reflected from the ground surface and other objects in the transmitted beam. Microwave sensors respond to changes in the vector sum caused by moving objects. The vector sum may increase or decrease, as the reflected signal may add in-phase or out-of-phase.

Bistatic microwave sensors are often installed to detect a human crawling or rolling on the ground across the microwave beam, keeping the body parallel to the beam. From this aspect the human body presents the smallest effective target to the bistatic microwave sensor. This has two important consequences for the installation of microwave sensors. First, the ground surface between the transmitter and receiver must be flat so the object is not shadowed from the microwave beam, precluding detection. The surface flatness specification for this case is +0, -6 in. (15.2 cm). Even with this flatness, crawlers may not be detected if the distance between antennas is much greater than 120 yards (109.7 m). Second, a zone of no detection exists in the first few yards or meters in front of the antennas. This distance from the antennae to the point of first crawler detection is called the offset distance. Because of this offset distance, long perimeters where microwave sensors are configured to achieve a continuous line of detection require that the antennas overlap one another, rather than being adjacent to each other. An offset of 10 yards (9.1 m) is typically assumed for design purposes; adjacent sectors must overlap twice the offset distance, for a total of 20 yards (18.3 m). Other site requirements are that the antenna height must be 18-24 in. (45.7 cm – 60.1 cm) above the sensor bed surface, and the slope of the plane of operation cannot allow more than a 1 in. (2.5 cm) elevation change in 10 ft. (3 m) from any point on the surface of the plane. Since the primary cause of nuisance alarms for bistatic microwave is standing water, the sensor performs best when the sensor bed surface is made of 4 in. (10.2 cm) of riverbed gravel, no larger than 1.5 in. (3.8 cm) in diameter, with a neutral color preferred for assessment purposes. If the gravel is larger, rain will still cause nuisance alarms. Crushed

rock that will pass through a 1 in. (2.5 cm) screen may be used. Smaller stones quickly fill up with soil and do not drain properly.

The detection volume for bistatic microwave sensors varies but is large compared to most other intrusion sensors. The largest detection cross-section is midway between the two antennas and is approximately 4 yards (3.7 m) wide and 3 yards (2.7 m) high.

Microwave sensors tolerate many environmental conditions without producing nuisance alarms, but some environmental conditions do lead to problems. Vegetation should be no higher than 1-2 in. (2.5-5.0 cm) tall in the area; it is better to have no vegetation at all. A nearby parallel chain-link fence with loose mesh that flexes in the wind may cause nuisance alarms. The flat plane required for crawler detection should have a cross slope for water drainage, and gravel should be used to prevent standing water on the surface of the zone. Heavy, blowing snow may produce nuisance alarms; snow accumulation reduces the probability of detection, especially for crawlers; and complete burial of an antenna in snow will produce a constant alarm. Defeats by bridging or digging under are difficult due to the extent of the detection volume. More sophisticated adversaries could use secondary transmitters as defeat methods.

Some form of fencing should be used around exterior bistatic microwave sensors to reduce the potential for nuisance alarms and to help maintain the carefully prepared area. These sensors are impractical where hills, trees, or other natural features obstruct the beam.

Exterior Video Motion Detectors (VMDs)

VMDs are passive, covert, line-of-sight sensors that process video signals from closed-circuit television (CCTV) cameras. The cameras may simultaneously be used for detection, surveillance, and alarm assessment. For 24-hour operation, lighting is required.

VMDs sense a change in the video signal level for a defined portion of the viewed scene. The portion could be a large rectangle, a set of discrete points, or a rectangular grid. Detection of human body movement is reliable except in fog, snow, heavy rain, or darkness. If video resolution is not sufficient to allow an operator to quickly determine the source of an alarm, the VMD will not perform well.

Outdoor use of VMDs may encounter many potential sources of nuisance alarms, such as apparent scene motion due to unstable camera mounts; changes in scene illumination due to cloud shadows, shiny reflectors, or vehicle headlights; and moving objects in the scene, such as birds, animals, blowing debris, and precipitation. Defeat tactics include taking advantage of poor visibility conditions and blending into the background (Ringler & Hoover, 1994; Matter, 1990). Video motion detection allows for alarm assessment by providing a video image to security personnel. The area of the image containing detected motion is

generally highlighted to allow a quick and appropriate response. A single camera can protect a large area, limited only by the field of view that the lens provides and camera resolution, or it can protect selected regions within the field of view through the use of masking (selecting only part or parts of the video scene that the VMD will protect, ignoring activity in the unmasked portions). Masking allows the VMD to discriminate between multiple zones created on one camera view. Depending on the performance desired, the system can be extremely sensitive, down to a single pixel of video. However, there is a tradeoff between the acceptable sensitivity and the rate of nuisance alarms; increased sensitivity results in an increase in the number of nuisance alarms.

Older VMDs use analog technology. These are still in production and can be very effective depending on the sensitivity settings of the system; however, they provide a limited ability to analyze an image and exclude false alarms, such as leaves on a tree or waves on a pool of water within the camera scene. Digital VMDs are becoming much more common. They are more expensive than their analog counterparts, but they address some of the shortcomings of analog VMDs. Digital VMDs use A/D (analog to digital) converters to sample the incoming video signal and electronically convert it to a digital value. The higher the resolution of the video signal, the greater the accuracy and performance of the VMD. High-resolution motion detection allows for longer detection zones, fewer cameras, and the detection of slower, smaller moving targets at longer distances.

Variables can be adjusted on a VMD to optimize detection capabilities and minimize nuisance alarms. As noted above, a masking feature will allow a variable number of detection areas and the modification of detection area dimensions. Target size and sensitivity can be adjusted to the particular application. Tracking features can be implemented to help in assessing video. Digital VMDs have some ability to adjust for gradual illumination changes in the environment and for some vibration in the camera. There is also a limited ability to discriminate between wind, rain, snow, blowing leaves, and small animals or birds. Even with the optimized adjustment of variables, low-end analog VMDs are best suited for the purpose of detecting any type of motion in the scene. On the other hand, high-end digital VMDs are generally good at false alarm rejection, very small (pixel level) detection, and estimation of the direction of motion, using the proper settings. They can also be very effective in low-contrast, poorly illuminated areas with slow movement.

VMD technology is best used in conjunction with other sensors. VMD developers are continually improving algorithms for use of the technology in a large range of applications. The use of VMD in interior applications has always been effective; with the advancement of digital VMDs, they are becoming increasingly popular in exterior environments, as well. Developments in recent years have extended VMD technology to three dimensions. A three-dimensional VMD (3D VMD) increases the detection capabilities and provides 3D information that can be used to assist in assessment decisions, such as intelligent filtering of nuisance

alarms, classification and targeting of moving objects, and volumetric sensing. VMD technologies are best suited for interior applications, providing good detection capability and low NARs. With respect to exterior VMD applications, further development is needed to reduce excessive NARs before deployment at high-security sites. If VMDs are used in conjunction with other exterior sensors, a lower sensitivity setting could be used to reduce nuisance alarms and still provide the operator with some visual assessment capability.

4.3.3 OTHER EXTERIOR SENSOR CONCEPTS

Technology Maturity

Decision makers in both government and commercial sectors are continually searching for technologies that will provide enhanced security within a finite budget. When new technologies hit the market, how does a decision maker (or a designer for that matter) determine if the technology is ready for deployment? A growing concern is that decision makers and designers of security systems may unknowingly accept significant risk if an immature security technology is fielded prematurely. One approach used to address this concern is a maturity model for security technologies.

The model includes the following:

- **Research.** The scientific basis is established, but the security application has not necessarily been identified. An example could be the discovery of the ferroelectric properties of lithium niobate, a material that has been used to sense IR energy in IR detectors.
- **Level I.** Concept feasibility is established in a laboratory demonstration.
- **Level II: Research prototype.** A prototype is hand-built in a laboratory, breaks a lot, and cannot withstand an operational environment.
- **Level III: Engineering prototype.** This prototype has about 90 percent functionality; reliability is improving.
- **Level IV: Field prototype.** This fully functional prototype works in an operational environment; produces reliable, repeatable results; is user-driven and accepted; and is ready to progress to full-scale production.
- **Level V: Commercial off-the-shelf technology (COTS).** Manufactured production units are available, with infrastructure in place for replacement parts and technology support.
- **Level VI: Performance testing.** This testing is done to establish performance metrics, such as probability of detection, NARs, vulnerability to defeat, performance

degradation factors, and sensor-to-sensor interference. This type of testing takes approximately 12 months for outdoor applications so that all weather conditions can be observed.

- **Level VII: Onsite testing.** This is done to determine actual performance in the desired operational environment, foliage, weather, and terrain, including integration into the site monitoring station.
- **Level VIII: Nontechnical maturity factors.** This is the site's concept of operations, addressing such issues as how the response force should use the information provided, how it should respond, and whether legal or policy issues prevent use of the technology.

Continuous Line of Detection

A perimeter is a closed loop around an area that needs protection. A worthy design goal is to ensure uniform detection around the entire length of the perimeter. Sensors must form a continuous line of detection around the perimeter, so hardware must be configured so that the detection zone from one perimeter sector overlaps with the detection zones for the two adjacent sectors. In areas where the primary type of sensor cannot be deployed properly, an alternate type of sensor is used to cover the gap.

Protection-in-Depth

In this context, protection-in-depth means the use of multiple lines of detection. At least two continuous lines of detection should be used in high-security systems. Some perimeter sensor systems include three sensor lines (such as a buried-line sensor, fence-associated sensor, and freestanding sensor), and a few have four. Using multiple sensor lines adds detection, increases reliability, and will fail safe (still providing some protection). In a multiple-line system, a sensor can fail without jeopardizing the security of the facility. Elimination of single-point or component failures ensures balanced protection even in adverse conditions.

Complementary Sensors

The perimeter sensor system can be made better not only with multiple lines of sensors but also with multiple, complementary types—for example, microwave and active infrared. This approach takes advantages of different sensor technologies' different PD, NAR, and vulnerabilities. The result is the ability to detect a wider range of intruders, keep operating during various environmental disturbances, and increase the intruder's difficulty of defeating the system.

Complementary sensors are an alternative to dual technology sensors, enabling the individual sensors to perform at their best and not be compromised by co-location and

filtering. Installing complementary sensors may be expensive, but it affords a higher protection level, which is why the practice is preferred in high-security applications.

Combinations of complementary sensors include microwave/infrared, microwave/ported coaxial cable, and ported coaxial cable/infrared. Detection patterns must overlap for the sensors to be complementary. A microwave/fence sensor combination would not be complementary because the detection patterns cannot overlap without serious nuisance alarm problems. Bistatic/monostatic microwave combinations would not be complementary since both are susceptible to the same defeat methods and nuisance alarm sources.

Priority Schemes

A disadvantage of multiple sensor lines is that more nuisance alarms may occur. If the system operator is overwhelmed, system effectiveness decreases. The reason is that the probability of detection decreases as the time to assess alarms increases. (This concept is explained further in Chapter 5, Video Subsystems and Alarm Assessment.) The assessment subsystem must help the operator evaluate alarm information. One aid is a computer that establishes the order of assessment for multiple simultaneous alarms. The computer sets a priority based on the probability that an alarm event corresponds to a real intrusion. The alarms are displayed to the operator in order of decreasing priority until all are assessed. This point is discussed in more detail in Chapter 7, Alarm Communication and Display.

Combination of Sensors

A sensor or sensor system should have a high probability of detection (PD) for all expected types of intrusion and a low nuisance alarm rate (NAR) for all expected environmental conditions. No single exterior sensor currently available meets both of these criteria perfectly; all have a limited detection capability and high NARs under certain environmental conditions.

The two main techniques for combining sensors are OR combinations and AND combinations. A system can include two or more sensors with their outputs combined by an OR gate so that an alarm would be generated when any sensor is activated. This combination is useful when sensors make up for each other's deficiencies; each sensor can detect particular types of intrusions. Sensors that detect aboveground, overhead, and tunneling intrusions should be combined by an OR gate. The nuisance alarm rate of the OR combination (NAR (OR)) is the sum of the NAR of each sensor. Because this combination results in an increased NAR, it is most useful for sensors that individually have low NARs.

If the sensors' nuisance alarms are not correlated, the nuisance alarm rate can be significantly reduced by combining sensors with an AND gate. For example, a seismic sensor and an electric field sensor do not give correlated alarms because they respond to different things. If both are

activated about the same time, it is probable they have detected an intrusion. Since the intrusion attempt may not activate two or more sensors simultaneously, the system can be designed to generate an alarm if two or more sensors are activated within a selected period. A long interval helps ensure detection of intruders moving slowly, but if the interval is too long, the NAR may not be reduced enough.

Detection probability of the AND combination ($PD(AND)$) is lower than the detection probability of each sensor. If detection performance is independent and coverage by sensors is redundant, the PD of the combination equals the product of the individual PDs. To ensure a reasonable detection probability for the system, the detection probability for each sensor must be high.

The nuisance alarm rate of the AND combination, $NAR(AND)$, is less than the nuisance alarm rate of each sensor. However, the AND scheme results in a lower PD because the intruder must only defeat one sensor.

Clear Zone

A perimeter intrusion detection system performs best in an isolated clear zone (or isolation zone). The clear zone increases detection probability, reduces nuisance alarms, and prevents defeat. It also promotes good visual assessment of the causes of sensor alarms.

A clear zone is usually defined by two parallel fences extending the entire length of the perimeter. The fences keep people, animals, and vehicles out of the detection zone, and the area between the fences is usually cleared of all aboveground structures, including overhead utility lines, as well as plants. When clear zones are bounded by two parallel fences, no sensors should be placed on the outer fence, where they would be susceptible to nuisance alarms from blowing debris and small animals. Video assessment outside the fence is difficult due to the inability of the camera to see through the fence fabric. Clear zones with multiple complementary sensors are generally reserved for use at high-security facilities, such as nuclear plants, prisons, military bases, or other government installations.

Sensor Configuration

Overlapping the detection volumes of different sensors in each sector enhances performance by creating a larger overall detection volume. Defeat of the sensor pair is less probable because a larger volume must be bypassed or two different technologies must be defeated. A third sensor can further enhance performance, not by overlapping with the first two but by forming a separate line of detection. Physically separate lines of detection may provide information useful for determining alarm priority during multiple simultaneous alarms. The order of alarms in a sector (or adjacent sectors) may correspond to the logical sequence for an intrusion.

Site-Specific System

A PPS designed for one site cannot be transferred to another, as every site has a unique combination of configuration and physical environment. The physical environment affects the selection of types of sensors for perimeter sensor systems. The natural and industrial environments affect nuisance alarm rates. Topography determines the shapes and sizes of the space available for detection, specifically the clear zone width and the existence of flat or irregular terrain. These factors generally suggest a preferred set of sensors. It is advisable to set up a demonstration sector on-site, using the sensors under consideration before committing to a complete system.

Tamper Protection

Both the hardware and the system design should aim to prevent defeat by tampering. In other words, the system should be tamper-resistant and tamper-indicating. Tamper switches should be placed on sensor electronics and junction box enclosures. Aboveground power and signal cables should be protected by being placed inside metal conduit. Alarm communication lines should use line supervision, which detects if lines have been cut, disconnected, short-circuited, or bypassed. If a sensor is relatively vulnerable to defeat, it should be placed, if possible, where an intruder must be in or pass through the detection volume to approach the receiver.

Self-Test

A perimeter sensor system's ability to detect must be tested regularly. Manual testing is recommended but takes much staff time. Remote testing of trigger signals, typically via a switch closure or opening, may be done through the central computer control system at random times. The control system checks whether an alarm occurred within a specified period and was cleared within another specified period. If not, there may be a hardware failure or tampering, and an alarm should be produced.

Pattern Recognition

Sensor technology is changing rapidly due to the development of inexpensive, powerful computers. These computers can now analyze sensors' signal patterns, looking for patterns that are particularly characteristic of an intruder. Using neural network or artificial intelligence software, computers can actually learn intruder signal patterns and then avoid nuisance alarms. Any sensor or combination of sensors (such as intelligent infrared and fence sensors) with a signal other than just off-on can have its signals analyzed.

Effects of Physical and Environmental Conditions

Numerous physical and environmental conditions can affect exterior detection systems, such as the following:

- topography
- vegetation
- wildlife
- background noise
- climate and weather
- soil and pavement

These conditions are different at every site.

Topographic features such as gullies, slopes, lakes, rivers, and swamps must be studied when designing an exterior detection system. Hills and slopes may need to be reduced through grading. To prevent seismic disturbances caused by running water, drainage systems may need to be designed to reduce water flow through gullies and ditches. The perimeter system should avoid lakes, rivers, and swamps, as few commercial sensors are suitable for use in water.

Vegetation can affect sensor performance both underground and aboveground. As trees or other plants blow in the wind, motion may be transmitted to their root systems and cause a seismic sensor to generate a nuisance alarm. Aboveground, large plants and trees can be used as cover by an intruder. They may also generate nuisance alarms. Vegetation may also attract small animals, creating more nuisance alarms. Problem vegetation can be controlled by mowing, removal, soil sterilization, or surfacing.

Large animals may collide with equipment, causing damage, and burrowing animals may eat through cable insulation. Birds and insects also cause nuisance alarms that may be difficult to assess. Dual chain-link fences and chemical controls may be used to control wildlife; however, local regulations may govern the use of poisons and repellents.

Sources of background noise, such as wind, traffic, electromagnetic interference, and seismic sources, can be discovered through a site survey along with information obtained from utility companies and plant engineering organizations on-site.

Wind can transfer energy to the ground through trees, power and light poles, and fences. If sensors are mounted on fences, they may generate nuisance alarms due to high winds and windblown debris.

Traffic from nearby roadways, railways, and airports creates nuisance alarms for seismic sensors. Roads should be kept smooth and the speed limit kept low to reduce the nuisance alarm rate. Seismic sensors are not practical near heavy air or rail traffic, which can cause seismic disturbances even at long distances.

Nuisance alarms due to electromagnetic interference can be triggered by lightning, radio transmitters, welding, and electrical transients. Such nuisance alarms may be reduced through shielding of the sources or the sensors.

Climate data should be obtained for the site. It is important to know the frequency, velocity, accumulation, and duration of hail storms, electrical storms, rain storms, and wind. Average minimum and maximum temperatures should also be noted, as should other weather and environmental conditions.

For buried seismic sensors, the seismic conductivity of the medium is the determining factor. It should be high enough to make seismic sensors effective, but not so high as to cause nuisance alarms. Wet soil generally has good seismic conduction, a characteristic that can lead to nuisance alarms from distant sources of seismic activity. Seismic magnetic sensors and seismic sensors may have to be embedded in or installed under areas paved with concrete or asphalt. A sensor embedded in pavement gains sensitivity if it is adequately coupled to the medium. If not coupled to the medium, it may be less sensitive than if it were installed in soil or buried under the pavement. Soil conductivity also affects the sensitivity of ported coaxial cable. Highly conductive soil reduces the detection volume of the sensor.

Lightning Protection

Because they are installed outdoors, exterior sensors are exposed to electrical storms at most sites. Lightning can disable, damage, or destroy the electronics used in sensor equipment. Three primary precautions apply to reducing lightning damage. First, signal cables should be shielded, whether by their internal cable construction or by using metal conduit. Second, a good ground system is needed. This requires elimination of ground loops and use of grounds at a single point. Third, at the ends of the cables, passive transient suppression devices can be installed. Because fiber-optic transmission cables are not affected by lightning, they have become popular for transmitting signals long distances outside a building.

Integration with Video Assessment System

In many perimeter security systems, CCTV is used for alarm assessment. For best results, the designs of the various systems or subsystems must be compatible. The reason is that video assessment tied to sensor activation greatly reduces the amount of time required to determine the alarm source, thereby maximizing the use of any remaining delay and increasing the chance of successful interruption of the adversary. Assessment may take place

over CCTV systems or be conducted in person. Video assessment offers the advantage of facilitating remote evaluation of the alarm condition, eliminating the need to constantly dispatch security officers to determine the cause of an alarm, possibly too late to make an accurate assessment. For maximum effectiveness, sensors must be placed so that when an alarm occurs, the camera viewing the zone can view the entire zone.

One trade-off involves the width of the clear zone. Sensor engineers prefer a wide area for installing their sensors to reduce nuisance alarms. Video engineers prefer a narrow area to assess so they can achieve better resolution. A compromise clear zone width is in the range of 10-15 yards (9.1-13.7 m).

Also to be balanced is the location of the camera tower within the clear zone. The camera must be able to view the entire area. The sensors must be far enough away from the camera towers to prevent nuisance alarms and distortion of the detection volume. Often the camera towers are placed 1-2 yards (0.9-1.8 m) inside the outer fence of the clear zone to prevent their use in bridging attacks by an adversary.

Integration with Barrier Delay System

Balanced, integrated PPSs usually incorporate barriers or access denial systems to provide delay time for video assessment of the alarm source and for the response force to respond to an intrusion. In many cases, the approach includes a barrier at the perimeter; however, the barrier should not degrade the performance of the sensors or obscure part of the camera's view. Perimeter barriers are usually installed on or near the inner clear zone fence. Such placement is important, preventing an intruder from tampering with or defeating the barrier without first passing through the detection zone. This placement ensures that response action can be initiated before the delay begins.

Procedures

As has been observed, an effective security system represents the successful integration of people, procedures, and equipment. For exterior intrusion detection systems, it is important to establish procedures related to installation, maintenance, testing, and operation. Current and new personnel will need training in these procedures, to learn the basics and to stay abreast of new technology.

The manufacturer's installation instructions may provide an appropriate starting point, but because many manufacturers cater to both the high- and low-end security market, users might be able to optimize sensor performance by going beyond the instructions. For example, several microwave manufacturers state that their units will operate at a separation of up to 300 yards. That may be so, but at that distance the sensor will not detect a crawling

intruder. Many fence sensor manufacturers suggest using a fence disturbance sensor around a corner, but it is not practical to assess that type of sensor zone.

All sensors and associated components need periodic maintenance. Calibration, sensitivity checks, alignment, and visual inspection should be performed regularly to keep the sensor components operating at their best. Poor maintenance affects PD and NAR and may make a system more vulnerable to defeat.

Operational tests, too, should be performed regularly to make sure the sensor element is contributing as expected to overall system effectiveness. The tests should be done both during the day and at night to verify that the sensor performs as expected against the design basis threat. Tests should be conducted for adversaries moving at various speeds: walking/running (slow and fast) and crawling. It also makes sense to test how slowly an object can move and avoid detection. Ideally, standardized tests should be used. Different testing methods are needed for different sensor types. For example, to test microwave sensors, one can use an aluminum sphere to simulate a crawling intruder. Such an approach produces more accurate, repeatable results than one obtains by performing actual crawl tests. For infrared sensors, a standardized test would be to measure attenuation factors.

It is important to develop contingency plans and procedures to implement in case a particular sensor or other equipment is lost. These plans should state when they will be used—for example, if two of the three perimeter sensors are lost. If the plan calls for compensatory measures (portable sensors, security officers), those measures should be specified. The specific procedures should be defined in advance and must be readily available to system operators for implementation.

After establishing procedures for maintaining, testing, and operating exterior sensors, it is time for site personnel to collect, store, and maintain key documentation. They will need to look for required, recommended, and troubleshooting procedures, as well as maintenance logs for each sensor, training records for all employees, and outcomes of any unique instances, such as causes of any false alarms.

4.4 INTERIOR SENSORS

In a system with administrative procedures, access controls, and material monitoring, interior intrusion sensors can be highly effective against insider threats. If interior intrusion sensors are correctly placed, installed, maintained, and tested, they can generate alarms in response to unauthorized acts or the unauthorized presence of insiders as well as outsiders.

As with exterior sensors, specific criteria for measuring the effectiveness of interior sensors are required. For example, the statement “Volumetric sensors shall detect an individual moving at a rate of 1 foot per second or faster within the total field-of-view of the sensor” is a clear and measurable specification for interior sensor performance.

Common sources of nuisance alarms for interior sensors include electromagnetic, acoustic, thermal, meteorological, seismic, and optical effects as well as wildlife (birds, insects, animals). False alarms are those nuisance alarms generated by the equipment itself (whether by poor design, inadequate maintenance, or component failure). Different types of intrusion sensors have different sensitivities to these nuisance or false alarm sources, as is discussed in detail later in this chapter.

An interior intrusion detection system is vulnerable to attack by both outsiders and insiders. Because insiders have authorized access to an area or facility, many perimeter exterior sensors are not in the detection path of the insider. Interior sensors, on the other hand, can still be useful for detecting insider theft or sabotage, as well as any attacks by outsiders.

Interior sensors are often placed in access mode during regular working hours, making them more susceptible to tampering by an insider. In many alarm-monitoring systems, access mode means the sensor alarms are temporarily masked so that alarms are not displayed at the alarm-monitoring station. An insider among maintenance personnel probably has the greatest opportunity and the technical skills necessary to compromise sensors or the system compared to other employees. Vulnerabilities created by a technically capable insider include reducing sensor sensitivity, shifting a sensor’s coverage area, or changing the characteristics of a zone area. These actions may not totally disable a sensor, but could create a hole in detection.

4.4.1 CLASSIFICATION

There are several ways of classifying the types of intrusion sensors. In this discussion, the following methods of classification are used for interior intrusion sensors:

- active or passive
- covert or visible
- volumetric or line detection
- application

Active or Passive

A useful way of looking at interior sensors and their interaction with the environment is to consider the sensors in two categories: active and passive. Active sensors transmit a signal from a transmitter and, with a receiver, detect changes or reflections of that signal. The transmitter and the receiver may be separated, in which case the installation is called bistatic, or they may be located together, in which case the installation is called monostatic. These active sensors generate a field of energy when the sensor is operating, and a very sophisticated adversary could use this field to detect the presence of the sensor prior to stepping into the active sensing zone.

Passive sensors are different from active sensors in that they produce no signal from a transmitter and are simply receivers of energy in the proximity of the sensor. This energy may be due to vibration (from a walking person or a truck), infrared energy (from a human or a hot object), acoustic activity (sounds of a destructive break-in), or a change in the mechanical configuration of the sensor (in the case of the simpler electromechanical devices). The distinction between active and passive has a practical importance. The presence or location of a passive sensor can be more difficult to determine than that of an active sensor; this puts the intruder at a disadvantage. In environments with explosive vapors or materials, passive sensors are safer than active ones because they emit no energy that might initiate explosives.

Covert or Visible

Covert sensors are hidden from view; examples are sensors that are located in walls or under the floor. Visible sensors are in plain view of an intruder; examples are sensors that are attached to a door or mounted on another support structure. Covert sensors are more difficult for an intruder to detect and locate, and thus they can be more effective; also, they do not disturb the appearance of the environment. Another consideration, however, is that visible sensors may deter the intruder from acting. Visible sensors are typically simpler to install and easier to repair than covert ones.

Volumetric or Line Detection

The entire volume or a portion of the volume of a room or building can be protected using volumetric motion sensors. An advantage of volumetric motion sensors is that they will detect an intruder moving in the detection zone regardless of the point of entry into the zone.

Forcible entry through doors, windows, or walls of a room can be detected using line-type sensors. These sensors only detect activity at a specific location or a very narrow area. Unlike volumetric sensors, line sensors only detect an intruder if he or she violates a particular entry point into a detection zone.

Application

Sensors may be grouped by their application in the physical detection space. Some sensors may be applied in several ways. There are three application classes for interior sensors:

- **Boundary-penetration sensors.** These detect penetration of the boundary to an interior area.
- **Interior motion sensors.** These detect motion of an intruder within a confined interior area.
- **Proximity sensors.** These can detect an intruder in the area immediately adjacent to an object in an interior area or when the intruder touches the object.

4.4.2 TYPES OF INTERIOR INTRUSION SENSORS

In the following discussion of interior sensor technologies, the sensors are grouped by their application. Excellent reviews of interior intrusion sensor technologies have been written by Barnard (1988), Cumming (1992), and Rodriguez and Matter (1991).

Boundary-Penetration Sensors

The most common sensors in this category include vibration and electromechanical technologies. Interior areas best protected by boundary penetration sensors include ceilings and floors of rooms as well as walls and doors.

Vibration Sensors

Boundary-penetration vibration sensors are passive line sensors; they may be either visible or covert. They detect movement of the surface to which they are fastened. A human blow or other sudden impact causes the surface to vibrate at a specific frequency determined by its construction. The vibration frequencies are also influenced by the impacting tool.

Vibration sensors include simple jiggle switches and complex inertial switches or piezoelectric sensors. Inertial switches use, as the sensing element, a metallic ball mounted on metal contacts. The sensor body is mounted on the vibrating surface, and the ball tends to remain stationary relative to the surface. When the sensor body is moved, the inertia of the ball causes the ball to momentarily lose contact with the mount, causing an alarm. An inertial sensor typically detects vibration frequencies of 2–5 kHz. In a piezoelectric sensor, the sensing element is also mounted on the vibrating surface and moves relative to the mass of the sensor body. This motion flexes the piezoelectric element, creating a voltage output that can be examined to detect an intrusion. A piezoelectric vibration sensor detects vibration frequencies of 5–50 kHz.

Glass-break sensors mounted directly on the glass they are protecting are vibration sensors, too (Figure 4-1). These sensors are specifically designed to generate an alarm when they detect the frequencies associated with breaking glass (normally above 20 kHz). Active glass-break sensors introduce a vibration into the protected glass and listen for the signal received by another transducer placed elsewhere on the glass. Breaking the glass causes the retrieved signal to change, causing an alarm. Active glass-break sensors cost more but produce fewer nuisance alarms.

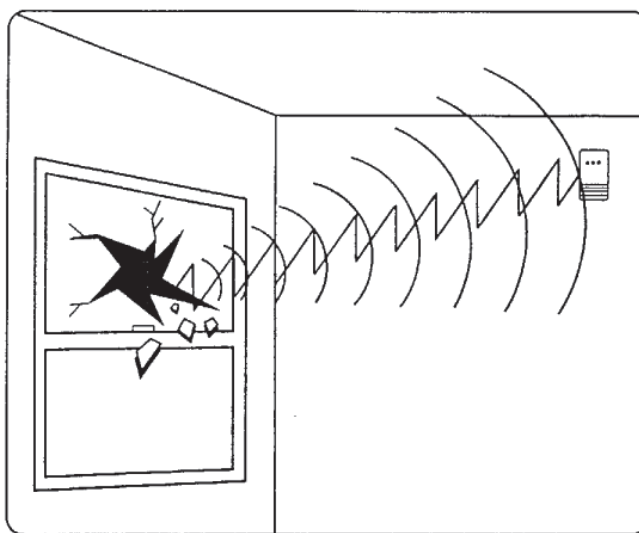


Figure 4-1
Glass-Break Sensor

Newer fiber-optic intrusion sensors also detect vibration. The passive line sensors may be either visible or covert. These sensors detect microbending of fiber-optic cable. Microbending is the minute movement of the cable due to vibration of the surface to which it is attached. A processing unit, part of the fiber-optic sensor, transmits light down the cable and receives it at the other end. Microbending detectably changes the light received at the end. The processing units typically allow for several user adjustments, such as low- and high-frequency filtering, amplitude filtering, and pulse duration and count. The adjustments are meant to reduce sensitivity to nuisance sources. However, before selecting a fiber-optic sensor for vibration detection, it is essential to consider vibrations from nearby machinery, vehicles, trains, and air traffic. It is possible to filter the nuisance frequencies, but doing so may reduce intrusion sensitivity.

Vibration sensors provide early warning of a forced entry. When applying vibration sensors, the designer must realize that the detector might generate nuisance alarms if mounted on walls or structures exposed to external vibrations. If the structures receive severe vibrations, vibration sensors should not be used. However, if the structures are subject to occasional impacts, it would be possible to use vibration sensors with a pulse accumulator or count circuit. These circuits allow a limited number of impacts to occur before signaling an alarm.

Electromechanical Sensors

Electromechanical sensors are passive, visible, line sensors. The most common type is a simple switch, generally installed on doors and windows, typically using a magnetic design consisting of a switch unit and a magnetic unit. The switch unit, containing a magnetic reed switch, is mounted on the stationary part of a door or window. The magnetic unit, containing a permanent magnet, is mounted on the movable part of the door or window and adjacent to the switch unit. When the door or window is closed, the spacing between the switch unit and magnet unit is adjusted such that the magnetic field from the permanent magnet causes the reed switch to be in the closed (or secure) position. When the door or window is opened and the magnet thereby removed, the magnetic field at the switch drops, causing the switch to move to the open (or alarm) position. These units can be defeated easily by placing a strong magnet near the switch unit, forcing the switch to the secure position.

In addition, a bias magnet in the switch unit can be adjusted to help prevent defeat. Magnetic sensors with bias magnets are generally called balanced magnetic switches (BMSs). Alternatives include multiple reed switches and multiple magnets; fusing and voltage breakdown sensing devices; and shielded case construction. Some units contain internal electromagnets for self-testing. Their complex interactions with the switch units increase the complexity of the unit and decrease its vulnerability to defeat.

BMSs provide greater protection for doors and windows than either magnetically or mechanically activated contacts or tilt switches. However, the actual level of protection is only as good as the penetration resistance of the door or window. These sensors only activate if the intruder opens the door or window for entry. Cutting through a door or window would bypass the BMS. Sample design criteria for a BMS might be as follows:

A BMS shall initiate an alarm whenever the door is moved 1 inch or more from the jamb . . . A BMS shall NOT initiate an alarm for door movements of ½ inch or less.

A relatively new type of magnetic switch is the Hall effect switch. It is completely electronic, without mechanical reed switches, and it requires power. It provides a higher level of security than balanced magnetic switches. Like other magnetic switches, it includes a switch unit and a magnetic unit. Relying on the Hall effect, devices in the switch unit measure and monitor the magnetic field strength of the magnetic unit. The Hall effect occurs when a current-carrying wire (or metallic strip) is exposed to an external magnetic field. When that happens, the magnetic field causes charge carriers to be accelerated toward one side of the wire, resulting in a charge separation across the wire. The amount and polarity of the charge separation is proportional to the magnetic field strength and magnetic polarity. The charge can be measured across the sides of a metallic strip. In a Hall effect switch, if the Hall effect devices measure enough magnetic field change, an alarm is generated. Both BMS and Hall effect sensors provide better protection against insider tampering and defeat than a simple magnetic switch. Moreover, a Hall effect switch is harder to tamper with and defeat than a BMS. An intruder needs more knowledge as the sensor technology progresses from simple magnetic switch to BMS and to Hall effect.

Another electromechanical sensor, called a continuity or breakwire sensor, is usually attached to or enclosed in walls, ceilings, or floors to detect penetration. The sensor consists of small, electrically conductive wires and electronics that trigger an alarm when the conductor is broken. The wires can be formed in any pattern to protect oddly shaped areas. Continuity sensors can even be made from printed circuit technology.

Breakwire grids and screens help detect forcible penetrations through vent openings, floors, walls, ceilings, locked storage cabinets, vaults, and skylights. Such sensors generate few nuisance alarms, since the wire must be broken to initiate an alarm. Breakwire sensors should be electrically supervised to decrease the chances of tampering. Since these sensors require a break or cut to detect, they can be defeated through the use of a jumper around a cut or by movement of the wire to allow penetration. Another version of a breakwire sensor uses optical fibers instead of electrical wire. The principle is the same—the optical fiber must be broken or damaged enough to stop or significantly reduce light transmission. These are fiber-optic intrusion sensors, but they are different and much simpler than the fiber-optic intrusion sensors described earlier under vibration sensors.

Interior Motion Sensors

By far, the most common sensors in this category are monostatic microwave sensors and passive infrared sensors.

Microwave sensors are active, visible, volumetric sensors. They establish an energy field, usually at frequencies on the order of 10 GHz. Interior microwave motion sensors are nearly always in the monostatic configuration, using a single antenna for both transmission and reception. Intrusion detection relies on the Doppler frequency shift between the transmitted and received signal caused by a moving object within the energy field.

The Doppler shift requires a sufficient amplitude change and duration to cause an alarm. The microwave transmitter sends out a known frequency, and if a higher or lower frequency is returned to the receiver, the target can be determined to be moving closer to or further from the sensor. Optimum detection for microwave sensors is achieved when the target is moving toward or away from the sensor, not across the detection zone. Microwave sensors should therefore be oriented so that the adversary is forced to move in that manner.

The shape of the detection zone, which is governed by antenna design, is like an elongated balloon. The antenna is usually a microwave horn, but it may also be a printed circuit planar or phased array. A detection pattern may be displayed in vendor documentation, but the true pattern may be different. The sensor may be defeatable if the target to be protected or the critical area falls within the concave portion of the true pattern.

Microwave energy penetrates most glass, plaster, gypsum, plywood, and other materials used in normal wall construction. Metal objects (large bookcases, desks, computer monitors, or fencing) in the protected area may cause shadow zones and incomplete coverage. On the other hand, because metal objects reflect the microwave energy, detection in potential shadow zones could improve.

The penetration ability of microwave energy presents advantages and disadvantages. An advantage is that an intruder can be detected by the microwave energy penetrating partitions within a protected volume; however, it would be a disadvantage to detect someone or something moving outside the protected area or even outside the building. Nuisance alarms would result. Special care should be taken when locating and directing the energy within the area requiring protection.

Other advantages of microwave detectors include these:

- invisible and inaudible detection pattern
- reliability and low maintenance requirements
- low cost for area of coverage

- high probability of detection
- immunity to high air turbulence and temperature and humidity changes
- availability of a variety of detection patterns

For all their good qualities, microwave sensors present a few disadvantages beyond those already described, including these:

- requirement for completely rigid mounting
- susceptibility to pattern drift
- tendency to reflect off metallic objects
- need for special considerations in areas with light construction (e.g., glass, plaster board, wood)

Monostatic microwave devices can serve as point sensors to provide limited coverage of a point or area in which other sensors may provide inadequate coverage or may be vulnerable to tampering. Monostatic microwave sensors are often used in the automatic door openers seen in supermarkets and airports.

Microwave detectors should be mounted near the ceiling of the area being protected. They should be aimed in the direction of desired coverage, yet they should avoid metal objects that might reflect microwave energy and cause nuisance alarms. If multiple microwave sensors are used in the same area, they must be set at different frequencies so they do not interfere with each other and cause continual nuisance alarms. Common sources of nuisance alarms for microwave sensors include movement of objects (nonhuman) within and outside the detection zone, movement of small animals or birds, and vibration allowed by poor sensor installation and mounting. The ionized gas in fluorescent lights can reflect microwave energy, causing nuisance alarms due to the 60 Hz rate of the ionization. Therefore, fluorescent lights should not be within the detection area of a microwave sensor. (However, some models have filters to ignore the Doppler shift created by fluorescent lights.) Microwave sensor vulnerabilities include slow-moving targets, absorption or reflection of microwave energy, blockage of the field of view (such as by stacking boxes or moving furniture around in a room), and motion along the circumference of the detection pattern.

Passive Infrared Sensors

Passive infrared (PIR) sensors are visible and volumetric. They respond to changes in the energy emitted by a human intruder, which is approximately equal to the heat from a 50-watt light bulb. Under the right circumstances, these sensors can also detect changes in the background thermal energy caused by someone moving through the detector field of view and hiding in the energy emanating from objects in the background. These systems typically

use special optical and electronic techniques that limit their detection primarily to an energy source in motion; therefore, reliance on background energy change for detection is discouraged.

Infrared radiation has four major characteristics:

1. It is emitted by all objects, in proportion to the object's temperature.
2. It is transmitted without physical contact between the emitting and receiving surfaces.
3. It warms the receiving surface and can be detected by any device capable of sensing a change in temperature.
4. It is invisible to the human eye. PIR sensors respond to infrared energy in the wavelength band between 8 and 14 nanometers (nm).

A passive infrared sensor is a thermopile or pyroelectric detector that receives radiation from the intruder and converts it into an electrical signal. The signal is amplified and processed through logic circuits, which generally require that the source of radiation move within the field of view of the sensor. If the signal is strong enough and the required movement occurs, the sensor generates an alarm. Detection is based on the difference in temperature between the intruder and the background; this difference is called the minimum resolvable temperature (MRT). Some manufacturers specify an MRT as low as 1° C (1.8° F).

A pyroelectric detector works because certain dielectric materials of low crystal symmetry exhibit spontaneous dielectric polarization. Infrared energy is focused onto the pyroelectric detector via segmented parabolic mirrors or Fresnel lens optics. These optics can provide either a single long conical field of view or a multiple-segment field of view. Long, single-segment sensors are used to protect corridors, and those with multisegments are used to protect large open areas. As with microwave sensors, the detection pattern is not a perfect shape. One should exercise caution when placing these devices. In addition, due to the operating principles of the device, a PIR is most effective if the target is forced to cross the detection pattern, entering and exiting multiple detection segments.

Passive infrared sensors are susceptible to nuisance alarms from birds and flying insects. Birds flying near a sensor can block the background energy from the thermal sensors, and if the birds' motions satisfy the alarm criteria, the result is a nuisance alarm. A nuisance alarm can also result from an insect crawling on the lens.

Infrared energy does not penetrate most building materials, including glass, so infrared energy from outside a protected building usually does not cause nuisance alarms. However, local heating effects inside the building could result from sources outside the building. For example, while glass and Plexiglas® window materials are effective filters for infrared energy

in the wavelength region of interest (8 to 14 nm), sunlight passing through windows can heat interior surfaces, which would then radiate energy in that band.

An infrared sensor should be installed away from heat sources, which could produce thermal gradients in front of the sensor's lens. An infrared detector should not be mounted over or near radiators, heaters, hot pipes, or other heating elements. Radiant energy from those sources can produce thermal gradients in the view of the detector's lens that might change the background energy pattern. The thermal gradients could cause nuisance alarms. An unshielded incandescent light that is within 3-5 yards (2.7-4.7 m) of the sensor could also cause an alarm if it burned out or went out due to loss of power.

PIRs offer several advantages:

- totally passive technology
- well-defined detection zones
- no interaction between multiple devices
- low to moderate cost
- relatively few nuisance alarms

They also have some disadvantages:

- moderate vibration sensitivity
- sensitivity variation due to room temperature
- line-of-sight operation with easily blocked field of view
- potential nuisance alarms from rapid temperature changes

Dual-Technology Sensors

Dual-technology sensors are active and passive, visible, and volumetric. They attempt to achieve absolute alarm confirmation while maintaining a high probability of detection. Absolute alarm confirmation is ideally achieved by combining two technologies, each with a high probability of detection and no shared susceptibilities to nuisance alarms. Most of today's dual-channel motion detectors (dual-technology) combine a microwave sensor with a passive infrared sensor. Alarms from the microwave sensor are logically combined with alarms from the infrared sensor in an AND-gate logic configuration. An alarm is produced only after nearly simultaneous alarms from both the active and passive sensors.

When dual-technology sensors are properly applied, and assuming each has a low nuisance alarm rate, such sensors usually have a lower nuisance alarm rate than single-technology sensors. However, when two sensors are logically combined using an AND gate, the probability of detection of the combined detectors is less than the probability of detection of the individual detectors. For instance, if a microwave sensor has a probability of detection of

0.95, and it is combined with an infrared detector that also has a probability of detection of 0.95, the dual sensor has the product of the individual probabilities of detection, or only 0.90. Microwave detectors have the highest probability of detecting motion directly toward or away from the sensor, but infrared sensors have the highest probability of detecting someone moving across the field of view. Therefore, because of that placement consideration, the probability of detection of the combined sensors in a single unit is less than if the individual detectors were mounted perpendicularly to each other with overlapping energy patterns and field of view. To optimize the probability of detection for combined sensors, it is better to use sensors that are separately mounted but logically combined. In high-security applications, a single dual-technology sensor should never be used instead of two separately mounted sensors. If dual-technology sensors are to be used, multiple sensor units should be installed, each unit offering overlap protection of the other.

Video Motion Detection

A video motion detector (VMD) is a passive sensor that processes the video signal from a CCTV camera. A single camera viewing the scene of interest can be used for detection, assessment, and surveillance. VMDs come in two main types: analog and digital. Analog VMDs monitor the camera signal and detect changes in brightness in the video scene. The size of the detection area (a percentage of total camera field of view) can vary widely. An external alarm is generated when brightness-related or other conditions (such as time) are satisfied. Once the alarm is generated, the section where detection occurred is highlighted on the CCTV monitor. Analog VMDs cost less than digital VMDs.

Digital VMDs, which are more sophisticated than analog VMDs, experience fewer nuisance alarms, making possible a wider use of video motion detection. Digital VMDs digitize the camera signal so it can be processed digitally. Generally, they divide a scene into several zones, elements, or cells, and process each cell separately. The cells are monitored for several types of changes: change in brightness or contrast, logical movement across adjacent cells, speed of motion across cell areas, size of objects within cells, and global changes across most or all cells. This processing allows better distinction between intruder movement and nuisance alarm sources. Digital VMDs can be used effectively indoors as long as one carefully considers nuisance sources within the area and employs proper lighting and good cameras and video transmission equipment. Interior nuisance sources include insects on or near the camera lens, flickering lights, pets, birds, and rats.

Camera characteristics affect detection capability and susceptibility to nuisance alarms. Low-contrast camera output cuts detection capability, and high noise levels from a camera can cause nuisance alarms. The cameras need sufficient, uniform light for proper operation.

VMD detects changes in the video brightness level, so any change can cause an alarm. Flickering lights, camera movements, and other similar movements can lead to high nuisance alarm rates, and very slow movement through the detection zone can defeat most VMDs. Many VMDs are effective for interior use because the interior space is free from snow, fog, traffic flow, and clouds, which can cause nuisance alarms.

Before installing VMD in a facility, it is important to perform tests on both a low-profile target, such as a crawler, and faster-moving, higher-profile targets, such as people walking or running. The tests should be performed under the lowest-contrast lighting condition expected. The following factors should be also be considered when selecting a VMD:

- consistent, controlled lighting (no flickering)
- camera vibration
- objects that could cause blind areas
- moving objects, such as fans, curtains, and small animals
- changing sunlight or shadows entering through windows or doors

Proximity Sensors

Two types of proximity sensors are pressure mats and capacitance sensors. Pressure mats are virtually obsolete, having been replaced by other technologies—principally PIRs. New installations are extremely uncommon, though the mats may still be in place in some facilities. Mats were typically installed under carpeting near doors, on stair treads or in other strategic locations. Operation involved initiation of an alarm when a weight of 5-20 lb./sq. ft. (24.4-97.6 kg/sq. m) was applied to the mat surface.

A version of the mat is still used, in conjunction with other detectors, to screen the numbers of persons or gross permissible weight through a portal. In these cases the mat or pad is actually a weight transducer and can be used at a remote card or keypad-controlled entry point to ensure that no person exceeding a programmed weight can gain access. When combined with distributed databases and unique PINs or cards, the authorized holder's actual weight, plus or minus a set margin, can be stored. When the PIN is entered in the keypad or the card inserted in the reader, the transducer-detected weight will be processed by the software entry algorithm.

Another type of proximity sensor, the capacitance sensor, is a large electrical condenser that radiates energy and detects change in the capacitive coupling between an antenna and the ground. In a typical installation, a capacitance sensor wire is connected to an object to be protected, such as a safe or file cabinet. An intruder who touches the object absorbs some of the electrical energy, disturbing the circuit and causing an alarm. Newer technologies, such

as PIRs, detect an intruder long before he or she reaches a protected object and have replaced many capacitance devices. However, if it is critical to limit the field of detection just to the protected object (a safe or file cabinet for example), a capacitance device may still be the preferred option.

Wireless Sensors

Radio frequency (RF) sensors are the most common type of wireless sensors. In the United States, they typically operate in the 300 MHz or 900 MHz bands, and some systems use spread-spectrum techniques for transmission. A typical RF wireless sensor system consists of sensor/transmitter units and a receiver. A sensor/transmitter unit includes both sensor and transmitter electronics in one package and is battery-powered. Battery life is advertised as two to five years, depending on the number of alarms and transmissions. Each sensor/transmitter unit is programmed with an identification code that is unique to it. Different systems have different transmission ranges and can accommodate different numbers of sensors transmitting to one receiver. In most systems the receiver can output alarm messages in several formats: RS-232, logic levels, or relay contact operation. To conserve battery power, the transmitters stay in sleep mode until an event requires a transmission. Events in this context are alarms, tampers, and state-of-health messages. Alarms and tampers are transmitted when they occur, and state-of-health messages are sent at set intervals to verify that the sensor is still present and operating. Such messages typically consist of battery status, alarm status, and tamper status. If the receiver does not receive the messages when expected, it will indicate a fault condition.

Most wireless systems use PIR, microwave, dual-technology, or magnetic switch sensors. They also typically contain a universal transmitter, which makes it possible to interface with other sensors or controls by monitoring the alarm contacts of the separate sensor.

Using an RF sensor system does raise some concerns, such as collisions, signal fade, and interference. Collisions occur when multiple signals, such as state-of-health signals, are received at the same time; in that case, no messages are read by the receiver. Fading may occur when the distance between the transmitter and receiver is too great or the path is blocked by material that shields the RF signal, such as large metal objects or metallic building siding. Interference occurs when other RF sources transmitting in the same frequency range overpower the sensor/transmitter's signal. Techniques such as spread-spectrum transmission and dithering the state-of-health timing can reduce these problems. Before placing and installing transmitters and receivers, it is beneficial to verify that there is a good transmission path that avoids possible interference sources.

4.4.3 OTHER INTERIOR SENSOR CONCEPTS

Environmental Conditions

Various environmental conditions can produce noise in the same energy spectra that the intrusion sensors are designed to detect. These outside noise sources can degrade sensor performance and may cause a sensor to generate an alarm even when an intruder is not present.

Several factors can degrade a sensor's performance. These conditions are often the cause of system vulnerabilities, and care must be taken to select and operate the appropriate sensor technology to achieve the desired security protection. Environmental conditions that can affect interior sensors include the following:

- **Electromagnetic energy.** Interior detection systems can experience interference from various sources of electromagnetic energy, such as lightning, power lines and power distribution equipment, transmission of radio frequencies, telephone lines and equipment, lighting, and computer and data processing equipment. Other sources include electric-powered vehicles (such as forklifts or elevators), television equipment, automotive ignitions, electrical machinery or equipment, intercom and paging equipment, and aircraft.

Details of the building or room to be monitored also affect the nature of the electromagnetic energy present. If the structure is made primarily of wood or concrete, neither of which provides electromagnetic shielding, there may be a high background of electromagnetic energy generated by sources outside the building or room. To minimize the effects of stray electromagnetic energy, it is possible to provide electromagnetic shielding to all system components (including all data transmission links) and ensure that all the components have a common, adequate electrical ground.

- **Nuclear radiation.** Nuclear radiation can damage various sensor components, such as semiconductors. Current systems cannot be made totally invulnerable to the effects caused by some radiation environments, but appropriate design, choice of components, and shielding can reduce system vulnerability. In general, neutrons degrade the performance of semiconductor devices and integrated circuits, depending on the total dose.
- **Acoustic energy.** Acoustic energy may come from sources inside or outside the area to be protected. Sources of acoustic energy that may affect the performance of interior sensors include meteorological phenomena; heating, ventilation, and air conditioning equipment; air compressors; television equipment; telephone electronic equipment; aircraft; vehicles; and trains.

- **Thermal environment.** Changes in the thermal environment may affect the performance of interior intrusion sensors. Such changes can cause uneven temperature distribution, leading to air movement within the area and expansion and contraction of buildings. Temperature changes may come from weather, heating and air conditioning equipment, machinery that produces heat, interior lighting, chemical and radioactive reactions, and fluctuations of sunlight through windows and skylights.
- **Optical phenomena.** Interior intrusion sensors may be affected by light energy from sunlight, interior lighting, highly reflective surfaces, and infrared and ultraviolet energy from other equipment.
- **Seismic phenomena.** Seismic phenomena affect interior intrusion devices by producing vibrations. Sources include earth tremors, machines or other equipment, vehicular traffic, trains, thunder, and high winds.
- **Meteorological phenomena.** Lightning, thunder, rain, hail, temperature, wind, earth tremors, high relative humidity, and sunlight can all adversely affect interior intrusion sensors.

Sensor Selection

It is important to consider the interaction among equipment, environment, and potential intruders before selecting intrusion detection technologies. Two important physical conditions that affect sensor performance are the construction of the building or room and the equipment and objects that occupy the space.

Because interior environments are usually controlled, predictable, and measurable, it is generally possible to find sensors that will perform acceptably in the environment. Nuisance alarm sources that may be present must also be considered, especially if motion detectors will be used. With an appropriate combination of sensors and sensor technologies, it is possible to achieve optimum performance. Adams (1996) provides a useful summary of operational issues.

Procedures

Various procedures can increase system effectiveness, such as two-person rules, sensor effectiveness testing, and good maintenance practices and documentation. When procuring sensors, one should select those that come closest to meeting performance goals and protection requirements while demonstrating compatibility with future systems.

The two-person rule requires that two knowledgeable people be involved in a situation or activity to prevent the compromise of facility security by a single insider. The two-person rule applies to functions such as granting access within the site and handling critical assets, information, or equipment. Each person involved in a two-person rule task must be able to

detect tampering by the other. The two-person rule will not work if the individuals involved relax the requirement because of long-term friendship or association.

Testing Mechanisms

For testing purposes, it can be useful if a sensor has an audible or visible alarm indicator that can be recognized from a distance of 10-35 ft. (3-10 m). (The indicator should be deactivated during operational use.) Walk tests should be conducted every day at first, and then spread out further if successful. All sensors should be performance-tested after maintenance. A sensitivity analysis or effectiveness test can be done to confirm a sensor's performance, verify sensor coverage, and check for blind areas created by changes in room layout. Self-test mechanisms (which may be separate devices or part of the sensor) make possible frequent operational testing of the sensor and alarm communication system. Self-testing should be activated randomly (Graham & Workhoven, 1987).

Installation and Maintenance

Installation and maintenance of sensors should be performed at least to the manufacturer's specifications, although there may be ways to optimize performance beyond the manufacturer's recommendations. Sensors and components should be inspected periodically to ensure that they conform to the required configuration and specifications. In these inspections, one should also look for possible alterations and modifications to components. Over time, acceptance tests, operational tests, and logs of maintenance calls on each piece of equipment will provide an idea of many and what kinds of spares to keep on hand. Spare parts must be inspected carefully before they are installed, and they should be kept secure during storage to deter tampering.

Inspection

After any maintenance, sensors should be inspected. All sensors monitored by a data-collection control panel should be walk-tested after any maintenance of the panel. An additional step for preventing changes that could degrade system performance is to require advance approval of plant modification plans by security personnel. Such modifications might include changing the location of detectors, adding objects that may cause nuisance alarms, and relocating large objects in the protected area. After remodeling, it may be necessary to readjust detector sensitivity.

Documentation

It is important to keep available documentation showing the theory of operation of the equipment, functional block diagrams, cabling diagrams, schematics, and parts lists providing manufacturers' and commercial equivalent part numbers. By consulting maintenance logs, one can monitor the reliability of equipment and problem components or areas.

System Integration

System integration is the process of combining technology elements, procedures, and personnel into a single system for providing security at a facility. Such integration requires a balance among hardware, personnel, and operational procedures. Like exterior sensors, interior intrusion sensors must be integrated with the display and control subsystem, the entry control subsystem, and delay mechanisms. This integration should include protection-in-depth, balance along all paths into the facility, and backup systems and contingency plans.

Line Supervision

Line supervision is a way to monitor the communication link between a sensor and the alarm control center. Using supervised lines between the sensor and host alarm system as well as continuously monitoring sensor tamper switches also helps protect against insider threats. The interior intrusion subsystem designer should be familiar with the range of available line supervision techniques, such as reverse polarity, sound monitoring, radio class C, steady direct current class B, tone, and digital classes A and AB. (Line supervision techniques are explained further in Chapter 7, Alarm Communication and Display.) If numerous interior sensors are connected to a single alarm processor, line supervision is required between the processor and each detection sensor.

4.5 SUMMARY

This chapter has examined exterior and interior intrusion detection sensors in terms of sensor classification and application, probability of detection, nuisance alarm rate, and vulnerability to defeat. The designer integrating individual sensors into an exterior perimeter sensor system must consider specific design goals, the effects of physical and environmental conditions, and the interaction of the perimeter system with a balanced and integrated PPS. Desired features include the use of a clear zone, proper configuration of sensors in the clear zone, alarm combination and priority schemes, tamper protection, and self-test capability. The design should be site-specific and suitable for the physical, environmental, and operational conditions that will be encountered. Finally, the exterior sensor subsystem should be well integrated with the video and barrier subsystems. The integration of individual sensors into an interior sensor system must consider the skill level of the intruder, the design goals, and the effects of environmental conditions, as well as the interaction of the interior system within a balanced and integrated PPS.

Security principles incorporated into a good intrusion detection system include protection-in-depth, use of complementary sensors, elimination of single-point failures, and integration of people, equipment, and procedures.

Sensor components and subsystems should provide a high probability of detection, low nuisance alarm rate, and low vulnerability to the defined threat. Other features include a fast communication system for sending and assessing alarms, good lighting and assessment systems, and a balanced system that provides adequate protection on all paths to the target perimeter.

REFERENCES

- Adams, D. (1996). *Operational tips for improving intrusion detection systems performance*. SAND 96-0468C. Albuquerque, NM: Sandia National Laboratories.
- Barnard, R. L. (1988). *Intrusion detection systems*, 2nd ed. Stoneham, MA: Butterworth Publishers.
- Cumming, N. (1992). *Security*, 2nd ed. Boston, MA: Butterworth-Heinemann.
- Fennelly, L. J. (1996). *Handbook of loss prevention and crime prevention*, 3rd ed. Boston, MA: Butterworth-Heinemann.
- Follis, R. L. (1990). *Stellar Systems Inc. series 800–5000 E-field sensor evaluation*. SAND 90-1039. Albuquerque, NM: Sandia National Laboratories.
- Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Boston, MA: Elsevier.
- Garcia, M. L. (2008). *The design and evaluation of physical protection systems*, 2nd ed. Boston, MA: Butterworth-Heinemann.
- Graham, R., & Workhoven, R. (1987). *Evolution of interior intrusion detection technology at Sandia National Laboratories*. SAND 87.0947. Albuquerque, NM: Sandia National Laboratories.
- Greer, G. (1990). *Vindicator VTW-250 test report*. SAND 90-1824. Albuquerque, NM: Sandia National Laboratories.
- Greer, G. (1990). *Vindicator VTW-300 test report*. SAND 90-0922. Albuquerque, NM: Sandia National Laboratories.
- Intrusion detection system handbook*. (1980). SAND 76-0554. Albuquerque, NM: Sandia National Laboratories.
- Matter, J. C. (1990). *Video motion detection for physical security applications*. SAND 90-1733C. Albuquerque, NM: Sandia National Laboratories.
- Ringler, C. E., & Hoover, C. (1994). *Evaluation of commercially available exterior video motion detectors*. SAND 94-2875.
- Stroik, J. (Ed.). (1981). *Building security*. Publication Number STP 729. Philadelphia, PA: American Society for Testing and Materials.
- Williams, J. D. (1988). *Exterior alarm systems*. SAND 88-2995C. Albuquerque, NM: Sandia National Laboratories.

Note: SAND documents may be obtained at <http://www.osti.gov/bridge/advancedsearch.jsp>.

CHAPTER 5

VIDEO SUBSYSTEMS AND ALARM ASSESSMENT

In recent years, closed-circuit television (CCTV) technology has improved greatly. The transition from analog to digital technology has changed the foundations of system design. In fact, the fast pace of development may lead a security manager to wonder how much new information he or she must master to stay current with CCTV trends. As the technology becomes better, smaller, and more reliable, the number of applications increases, but fortunately the theory of CCTV application remains the same.³ This chapter discusses the theory of designing CCTV security systems, the changing technology, and guidelines for choosing equipment.

In designing a CCTV application, security managers should keep in mind the following points:

- CCTV is a visual tool of security and should be applied accordingly.
- The application dictates the equipment, not the other way around.
- No matter what, the equipment of the system will become obsolete. However, obsolete does not necessarily mean ineffective or out-of-date for the application.
- If a system is obsolete but still performing well, it is because the original application was correctly designed to meet the performance needs.
- CCTV systems should always be designed with potential future growth or changes to the needs of the application in mind.

³ Most of this chapter comes from *The Professional's Guide to CCTV* by Charlie R. Pierce, published by LeapFrog Training & Consulting, and is used with permission.

5.1 THEORY OF VISUAL SECURITY

Video motion is an illusion. It is a sequence of images flashed in front of the eye at a rate that the brain perceives as movement. Blank spaces between images add smoothness to a scene and bolster the illusion of motion. In analog systems, the monitor paints individual lines (horizontal sweep lines) across the screen one at a time, from left to right, top to bottom. It also paints an equal or greater number of lines up and down (vertical sweep lines). Where the horizontal and vertical sweep lines meet, one finds a point or pixel of energy. The more pixels a monitor displays, the better the overall resolution or quality of detail within the image. Vertical resolution is restricted by NTSC⁴ or PAL⁵ standards. Horizontal resolution is limited only by the camera imager, monitor, and bandwidth of the transmission and recording medium. Consequently, the most common measurement of the quality or detail in an analog image is horizontal resolution. The more lines of horizontal sweep on a screen, the better the detail in the video picture.

All analog CCTV monitors and cameras employ a two-to-one (2:1) interlace pattern. The monitor first paints the odd-numbered horizontal sweep lines of the image and then resweeps the screen with the even-numbered horizontal sweep lines. This process creates 60 fields (half pictures) of information per second in NTSC and 50 fields per second in PAL. Combining one odd field and one even field of video information produces one complete frame or picture of analog video. In NTSC, for example, the viewer sees 30 complete frames each second.

Digital video technology does away with three things. First, digital technology does not use 2:1 interlace to produce a single image on a screen. Digital images are presented on the monitor as a full grid of small, colored squares or pixels. Second, real-time digital video may not be represented by “30 frames” per second. One stills measure in terms of images or frames per second (ips or fps), but real time is based on the needs of the application on a camera-by-camera basis. Perhaps 20 percent of cameras in a system may be recording at a different frame rate from the other cameras. Third, video is no longer held to NTSC or PAL standards but instead to the various digital standards established for visual media. Although digital standards vary around the world, all digital knowledge is being standardized on a universal basis. Therefore, the video recorded or stored in digital standards in the United States may be equally usable in the UK, Mexico, or African nations.

⁴ NTSC stands for National Television Standards Committee and is the standard for resolution in the United States, Japan, and parts of Latin America. The NTSC standard is 60 fields per second at 525 vertical lines.

⁵ PAL stands for phase alternation line and is the standard for resolution in Europe, Australia, China, and parts of Latin America. The PAL standard is 50 fields per second at 625 vertical lines.

5.2 USES OF VIDEO SUBSYSTEMS IN SECURITY

CCTV systems are meant to be visual assessment or visual documentation tools, nothing more. Visual assessment refers to having visual information of an identifying or descriptive nature during an incident. Visual documentation refers to having visual information stored in a format that allows the study or review of images in a sequential fashion. In addition, visual documentation includes various embedded authenticity points, such as a time/date stamp or character generation.

There are only three reasons to have cameras in security applications:

- to obtain visual information about something that is happening
- to obtain visual information about something that has happened
- to deter undesirable activities

Satisfying the first two reasons requires the right combination of camera and lens. One should base the choice of camera first on the camera's sensitivity, second on its resolution, and third on its features. Sensitivity refers to the minimum amount of visible light that is necessary to produce a quality image. Resolution defines the image quality from a detail or reproduction perspective. The camera's features are the aspects that give one camera an advantage over another, such as video motion detection, dual scanning, and built-in character generation. The camera should be chosen before the lens.

It is common to use different camera models within the same system. However, it is important to verify compatibility of language and format when using cameras that were produced by different manufacturers within the same system. Phasing and sequencing problems most often arise when cameras from several manufacturers are used in one system. Incompatibility with operations, viewing, or storage and playback mostly affect digital systems.

Lenses determine what amount and type of image will ultimately appear on the monitor. A lens should be chosen for its ability to produce the desired identification information. The three theoretical identification views of a CCTV system are subject identification, action identification, and scene identification.

5.2.1 **SUBJECT IDENTIFICATION**

This is the ability to identify something or someone within the scene beyond a shadow of a doubt. An illustration of subject identification would be to view a \$100 bill from a distance of 3 feet (0.9 m). A person with mediocre eyesight should be able to identify the item as a \$100 bill without a doubt. This sort of identification, like CCTV identification, does not allow the viewer to touch, smell, or taste the object (and usually not to hear it), so the visual information must be sufficient for identification. If the \$100 bill were moved to a distance of 30 feet (9 m), a person with normal eyes would not be able to identify it specifically.

Another demonstration of subject identification shows how the camera's angle of view affects the results available from a CCTV system. A person standing on a desk, looking directly down onto the top of various peers' heads as they come and go from an office, may not be able to identify the people—especially if the viewer does not know the people. Identification from such a steep angle is even more difficult with CCTV images. Thus, subject identification depends first on the size and detail of an image and second on the angle of view.

Finally, for subject identification, the object should occupy at least 10 percent of the scene's width. The average person is 2 ft. (0.6 m) wide. Therefore, to show the full body and still make it possible to identify the person beyond a shadow of a doubt, the scene can be no more than 20 ft. (6 m) wide. This guideline is based on a minimum 325 horizontal line resolution, which is television quality. The designer must pay extra attention when using newer digital storage or projection systems. Quite often, the image on the screen has a considerably lower resolution. Although the image might appear sharp in its 1-2 in. (2.5-5.0 cm) square on a computer screen, it may become indistinct when enlarged to a 5 x 7 in. (12.7 cm x 17.8 cm) print.

5.2.2 **ACTION IDENTIFICATION**

This form of identification captures what happened. For example, a person pins a \$100 bill to a wall and steps back to watch it. A second person enters the room, and the first person closes his or her eyes. Now the \$100 bill is gone. The first person saw the second person enter the room but did not see him or her take the money. Thus, the first person does not have enough evidence to prove that the second person took it.

The lesson is that CCTV systems should be automated through a trigger. A system can be programmed to respond to video motion detection, pressure on a floor mat, or the breaking of a photoelectric beam. The triggered response might be to improve the resolution or the number of images recorded per second. The response might also be to bring the image to the attention of a guard. With automated triggering, the system records important actions and captures useful evidence.

5.2.3 SCENE IDENTIFICATION

Each scene should stand on its own merit. If a security officer witnesses a fallen employee via CCTV, he or she might respond according to procedure and call paramedics. However, if the security officer does not read the character generation on the video screen, he or she might send the paramedics to the wrong location—that is, to a place that looks like, but is not, the location where the employee fell. Scene identification is an all-important but often missed form of identification.

The angle of view and the pixels per foot or meter dictate the placement and selection of cameras and lenses.

5.3 ANALOG SYSTEM COMPONENTS

An analog video system consists of three main components:

- camera (used to transform a reflected light image into an electronic signal)
- transmission cable (used to transmit the electronic video signal from the camera to the monitor)
- monitor (used to translate the electronic video signal into an image on a screen)

Other parts of an analog video system may include the following:

- **Pan or pan/tilt unit.** If the user wants the camera to move, a pan or pan/tilt unit is in order. A pan unit moves the camera from side to side. A pan/tilt unit moves the camera from side to side and up and down. Pan/tilts can be an important part of a CCTV system, but in most applications it is more cost-effective to use several fixed cameras instead of a single pan/tilt camera. Today's pan/tilt systems, for the most part, are built into a single unit protected inside a dome (call an auto-dome). Originally, pan/tilts helped cut system costs by reducing the number of cameras needed. However, today it is possible to buy several fixed cameras for the cost of one pan/tilt system. Therefore, pan/tilts are now typically used mainly in systems that use zoom lenses, that interface with alarms,⁶ or that employ pre-positioning.⁷

⁶ In alarm interfacing, an event (such as tripping of a door contact, photo beam, or motion detection system) is used to trigger a response from the camera system. The response may be to call up an image to a specific screen or multiple images in a series or layout on the screen or to trip a recording system to a higher frame rate of recording. Alarm interfacing cuts down on the amount of times spent watching images.

⁷ Pre-positioning is a mechanical or electronic setting that directs the camera to return to a particular pan/tilt and zoom position when a signal is tripped

A system designer should not add a pan/tilt without carefully considering the application's demands, as pan/tilt systems may increase requirement for additional staff time.

- **Controller.** A controller commands a function of a pan unit, pan/tilt unit, or automatic lens. In selecting a controller, it is important to remember that the application chooses the equipment, not the other way around. Once the application is decided, the equipment will fall into place.
- **Switcher.** To show the displays from several cameras on one or more monitors, a system generally requires a switcher. Video switchers save money by making it possible to use more cameras than monitors. They come in many types. With a passive, four-position switcher, the user pushes a button and an image appears on the screen. Dwell time is the time a sequential switcher automatically switches from camera to camera. It is not a factor when a switcher with more inputs than cameras is attached. A sequential switcher automatically switches from camera to camera. A quad splitter displays four images on a single screen. A user with a sequential or quad splitter should consider upgrading to a multiplexing switcher, which can interact with the system's video recorder to store more information per camera. A multiplexing switcher can also play back video streams separately or in quad format, according to need. Another type of switcher is the matrix switcher, which can organize large groups of video inputs and outputs and integrate them with alarms and viewing options.
- **Lens.** If it focuses light onto a chip or tube within a camera, it is a lens. Lenses come in a variety of sizes, allowing many different fields of view (the width and height of the scene). The proper lens makes it possible to capture an image that provides the right amount of identification within the overall scene.
- **Video transmitter/receiver.** This type of device allows the video signal to be transmitted via cable, phone line, radio waves, light waves, or other means. It is common to use several video transmission methods within a single system. Coaxial cable is the most common medium but not necessarily the best for all cameras within a system. It is possible to have a long, outside run on fiber-optic cable in the same system that uses two-wire (twisted pair) transmission as its primary transmission method.
- **Amplifier.** Amplifiers strengthen the video signal for long-distance runs, but one should avoid amplifiers when possible, as most installers do not have the proper tools to balance amplifiers into the system. If a system uses a coaxial cable run that is long enough to justify the use of an amplifier, it may be better to replace the coaxial cable with fiber-optic, microwave, or two-wire transmission.
- **Video recorder.** This device retains the video information on a magnetic tape, CD, DVD, hard drive, or other medium. The right form of recording is determined by the need. Recording features include time-lapse, event-triggered, 24-hour, 72-hour, and more.

Once the designer understands the basics of each preceding category, it is possible to design a simple or complex system on paper and have it work in the field.

The key points to remember are these:

- Once simplified, the most complex of electronic systems can be managed by almost anyone.
- The application drives the choice of equipment.

5.4 DIGITAL SYSTEM COMPONENTS

The world of analog CCTV has faded into the background behind digital. Even the name, CCTV, will change. A fully digital environment will use terms like digital imaging system (DIS) or visual imaging system (VIS).

The three main parts of a digital video system are as follows:

- camera
- digital electronic signal carrier, such as Category 6e (Cat 6e) cable or digital network
- PC with viewing or recording software (sometimes accessible via a Web browser or remote video device, such as a smartphone or tablet computer)

Other parts of a digital video system include the following:

- **Digital electronic scanning software.** These programs allow a fixed, megapixel camera to appear as if it were mounted to a mechanical pan/tilt device. This is accomplished by scanning across the imager in a predetermined path as opposed to physically moving the camera. It is also possible to deploy digital cameras with traditional, mechanical pan/tilt devices inside a dome enclosure.
- **Controller.** For the most part, digital controllers are computer programs installed on a server, personal computer, or handheld device. Digital controllers can work with a joystick or be controlled via pointing and clicking with a computer mouse. Many Internet protocol (IP) cameras⁸ and digital systems use proprietary graphical user interfaces (GUIs).⁹

⁸ Analog cameras are sometimes marketed as being “digital” if they have digital effects. Fully digital cameras may also be called Internet protocol (IP) cameras. IP is a language for digital transmission

⁹ A graphical user interface is the visible screen (like that presented by Microsoft Windows) used for controlling a computer.

- **Switcher.** A digital CCTV system can use three types of switching. First, it might use a high-speed, analog-to-digital converter (encoder) that accepts multiple analog signals and outputs a single, multiplexed¹⁰ digital signal. Second, the system might use a high-speed digital switcher that in essence is a multiplexer. Third, some digital video recorders (DVRs) contain built-in multiplexers. Once a camera is connected to a PC, the video information is stored on a hard drive, CD, DVD or on the Internet. The information is not necessarily multiplexed but may be stored as individual sequences or image files.
- **Lens.** The lens is one of the few elements of a video system that is not converting to digital. However, because of the capabilities of IP cameras and other control points within an IP system, various functions of the lens (e.g., auto-iris, zoom, and focus) can be automated so they do not require setup by a field technician and do not have any moving parts.
- **Video transmitter/receiver.** Ethernet is the most common transmission medium for digital systems, though it is not necessarily the best application for all cameras within a system. It is possible to have a long, outside run on fiber-optic cable in the same system that uses two-wire transmission as its primary transmission method. It should be noted that RG-59/U, RG-6/U, and RG-11/U coaxial cables can be used to carry a digital video signal via specialized signal modification equipment.
- **Amplifier.** For the most part, amplifiers in the digital world are repeaters. Since digital signals are binary codes, the signal itself does not require amplification. It is the carrier¹¹ that must be maintained. A signal is received, and an exact copy with a renewed carrier strength is emitted. The maximum cable length for digital transmissions is 100 meters or 312 feet unless using wireless, microwave, fiber optics, modified coaxial cable systems, or another medium designed for long-distance transmissions.
- **Video recorder.** Although DVRs made a huge entrance early in this millennium, many larger applications proved that stacked or multiple DVRs were not necessarily the way to go. DVRs have fixed inputs, accepting signals from 4, 6, 8, 12, 16, or more cameras. However, most DVRs are not true digital recorders, as they only accept analog inputs and their outputs are equally analog. In larger systems, DVRs are being replaced by massive hard drives or digital database storage systems.

¹⁰ Multiplexing combines the signals from several video cameras into a single data stream. The combined signal does not carry the full number of frames from each camera. If a system has three cameras, each producing 30 frames per second, a multiplexed signal of the three would carry 10 images per second from each.

¹¹ The carrier is the electronic signal on which the digital stream or sequence of electronic commands rides.

5.5 SYSTEM DESIGN

CCTV systems are not as complicated as they appear. System design can be addressed by following a few simple rules:

- **Keep the system in perspective.** CCTV systems contain only three major components: camera, cable, and monitor. Any other item is peripheral.
- **Let the application choose the equipment, not the other way around.** Salespeople may claim their equipment will handle all the user's needs—without even asking what those needs are. The user should first determine his or her needs and only then select equipment.
- **Design generically.** The best system design does not necessarily specify models or brands but remains open based on site or scene requirements
- **Design for the best option first.** Anything can be done with the right resources. It is best to design the application before establishing a budget. After the design is completed, the designer should calculate its cost and then, if necessary, remove some elements.
- **Don't feel the system must be built all at once.** Once the design is completed, the installation may be stretched over several budget years. The key is to work with equipment that is solid, is proven, and will most likely remain available for the next several years.

The user should take the following steps before putting the new system out for bid:

STEP 1: WRITE THE PURPOSE OF THE PROPOSED CCTV SYSTEM.

If the purpose is to monitor the back aisle of a store, little advance layout is necessary to make a viable system. If the intention is to cover several locations in several complexes, more work is required. In any system, over time, parts of the system may end up serving purposes other than security. The designer should consider the many ways in which the system might be used. In the process, he or she may discover unknown options. For example, it might be possible to divide the system so that some segments serve security purposes and others monitor traffic or product flow. It may then be possible to split the CCTV budget with other company departments.

The bottom line is to write out the purpose. Having it written out will keep the designer on track and allow the upgrade to change in a logical way if necessary.

STEP 2: WRITE THE PURPOSE OF EACH CAMERA IN THE SYSTEM.

To define the purpose of each camera, it is necessary to weigh the security risk of each area to be viewed. For a high-security area, it may be worthwhile to interface the CCTV system with an alarm device, such as a door contact, microwave motion detector, photo beam, or video motion detector. In a low-security area, alarm interfacing may not be necessary and recording the video signal as a backup reference may be the best option.

Another issue is whether the unit should be visible or covert. Camera visibility can, to a limited degree, deter certain nonchalant crimes or crimes of convenience in shopping centers or malls. Covert cameras, on the other hand, often promote security while allowing individuals to be comfortable in their surroundings. If covert applications are to be used, the security manager must make sure to respect privacy rights.

STEP 3: DEFINE THE AREAS TO BE VIEWED BY EACH CAMERA.

In this step, one defines the proposed cameras' actual view in terms of both height and compass points. For example, the designer might write that camera #1 will be 30 ft. high on the northeast corner of building 5, looking at the west gate, and that camera 2 will be mounted above the west exit in the north hallway of building 6, looking east.

STEP 4: CHOOSE A CAMERA STYLE.

The choice of camera style should be based on sensitivity, resolution, features, and other design factors.

Sensitivity. This is the minimum amount of light required by the camera to produce an image. The first consideration in choosing a camera is the lighting in the area. Is it bright or dim? Is it constant or variable? Does the location contain lights that could brighten the scene at night or during cloudy days? Does the viewing area contain large windows? Are the windows covered with heavy curtains? Are the curtains closed during the day, or are they opened according to the varying light conditions outside? Will the proposed scene have a bright background that silhouettes the people being surveilled?

For interior cameras, sensitivity is not usually a major concern unless, for example, the areas viewed by those cameras are not lighted adequately at night. If the system design includes several exterior cameras, a lighting study may be in order. Such a study is not especially difficult but requires some training and a good light meter. If additional lighting is necessary for nighttime operation, one can consider both visible and infrared (IR) lighting. IR light is not visible to the human eye, but many cameras view it the same way humans view visible

light. If the decor of a building or the presence of neighbors forbids the installation of visible lighting, IR lighting may be the solution.

Cameras come in three basic sensitivities: full-light, lower-light, and low-light. Full-light cameras are designed to produce good, even pictures indoors under full, consistent or minimally variable lighting conditions. Lower-light cameras are designed to produce good, usable video images under lighting conditions equivalent to dusk or dawn. Low-light cameras are designed to produce images where little or no light exists. Full-light cameras are usually the least expensive, lower-light cameras are in the middle to high price range, and low-light cameras are the most expensive.

Resolution. This is a critical measure of the picture quality, specifically the number of horizontal scan lines or digital pixel arrays that the camera captures. The cameras selected must capture video at a resolution sufficient to produce images with enough detail to produce viable visual evidence. Both the lens and camera should be chosen for their ability to produce the desired identification information. The improvements in image quality made available by digital visual imaging have increased the number and types of identification available through video surveillance. With analog, one still refers to the number of horizontal lines in an image to determine the identification level of the final resolution of an image. However, with digital imaging, one refers to the number of pixels per foot or meter at the point of recording for identification levels. Thanks to high density (HD)¹² and megapixel¹³ technology, one can now perform extreme identification of subjects that were impossible to discern with a standard analog camera in the past. Instead of the three levels of identification available to analog cameras, digital imaging makes possible seven theoretical identification views:

- **General.** Clothing and colors not distinguishable. No blowup for detail of person-sized targets. 5 pixels/ft. (16 pixels/m).
- **Monitor.** General human or vehicular traffic flows. No serious detail upon blowup. 7 pixels/ft. (23 pixels/m).
- **Detect.** Person-sized targets large enough to be detected but not identified. No significant detail on blowup. 11 pixels/ft. (35 pixels/m).
- **Observe.** Clothing and colors start to become distinctive. No good detail on blowup of person-sized targets. 18 pixels/ft. (58 pixels/m).

¹² High density video (HDV): a term used with high resolution cameras, images, or monitors. HDV does not imply megapixel technology but complies to the international standards of HDV TV at 1080p (1,080 pixels on a 16:9 screen ratio). Additionally, HDV allows for very low bandwidth video streaming and storage.

¹³ *Megapixel*: a term used to refer to a camera that has an imager that is made up of millions of pixel points. Megapixel technology allows for extremely wide views with equivalent 4 CIF or better resolution.

- **Recognize.** High degree of accuracy identifying and separating known individuals. Good detail for general blowup of an image. 35 pixels/ft. (118 pixels/m).
- **Subject identification.** Establish identity of individuals beyond shadow of doubt. Excellent image blowup. 46 pixels/ft. (150 pixels/m). In analog view, subject equals 20 percent of the overall scene width at the point of recording based on a minimum 325 horizontal line resolution.
- **License plate identification.** Identification of license plates and similar-sized objects with excellent detail on blowup. 70 pixels/ft. (231 pixels/m).
- **Facial recognition.** Extreme detail. Excellent resolution for image blowup. 88 pixels/ft. (289 pixels/m).

Features. Features of CCTV cameras include the following:

- **Automatic gain control (AGC).** An AGC circuit is built into most cameras that have a wide range of sensitivity. This is an internal video-amplifying system that works to maintain the video signal at a specific level as the amount of available light decreases. AGC was originally designed to ensure that a camera continued to produce a consistent image as it panned through a shaded area. All cameras mounted outside should have the AGC switched on. Many charge-coupled device (CCD) cameras sold today do not give an option of turning the AGC off.

Unfortunately, AGC increases noise in the video picture by a factor of 10, degrading the video quality dramatically in low-light situations. However, AGC is extremely useful when the camera swings into an area that is just below minimum light requirements, allowing the security person to continue viewing in areas that normally would go black.

A camera's AGC sensitivity should not be confused with its general sensitivity. AGC sensitivity, which provides a usable but low-quality image, is sometimes quoted as a way to make cameras appear, on paper, more sensitive than they really are.

- **Electronic shuttering.** Electronic shuttering (manual or automatic) refers to a camera's ability to compensate for light changes without the use of automatic or manual iris lenses. The feature is equivalent to using eyeglasses that turn dark when exposed to bright light. Such glasses reduce the amount of light that reaches the eye, just as electronic shuttering reduces the amount of light that reaches the camera's imaging. With electronic shuttering, a camera can either work in a wide range of light without an auto-iris lens or produce high-speed images to capture fast-moving objects.

With the introduction of the IP camera and the digital hybrid, electronic shuttering changed. No longer is the image darkened as a whole. Now each pixel on the CCD or imager is analyzed and filtered. If the image has a bright spot, the electronic shutter

dims the points of extreme brightness without affecting the overall performance of the camera or reducing its sensitivity. This can all be done with or without an auto-iris lens. However, it is still advisable to field test the equipment to verify its claimed specifications.

- **Backlight compensation.** One of the hardest tasks for a CCTV camera is to view a subject in front of a bright background. The most common such situation involves looking at someone standing in front of a glass door to the outside. Manufacturers have developed various methods for meeting that challenge:
 - **Auto-iris lens.** The most common tool for controlling the brightness of an image focused onto a chip is the auto-iris lens. Unfortunately, many CCTV system designers misunderstand how an auto-iris lens works. This ignorance often leads to camera applications that are beyond the scope of the camera's ability, resulting in silhouetted or extremely dark images.

All analog electronic, auto-iris lenses are designed to respond to the average amplitude of the raw video signal produced by a camera through a video sampling circuit. As a CCD (imager) is exposed to more light, the raw video signal increases. As the light decreases, the raw video signal decreases. The auto-iris lens, if installed properly, ensures that the video image remains at an average of one volt peak-to-peak (vpp) under optimal lighting conditions. As the video signal increases or decreases, the auto-iris lens closes or opens in direct proportion. For normal lighting conditions and fluctuations, this method of control works well. However, since the video sampler works on averages, the camera staring into bright areas will compensate for the brightness. This leaves all other portions of the image dark or in silhouette. That is why auto-iris lenses cannot keep up with this everyday problem application.

- **Masking.** This method of digital interfacing with the video signal is built into specific cameras and controllers. Masking divides the video image into grid sections. Next, various sections are programmed to be ignored. Then the grid overlay is turned off and the image is viewed without obstruction.
- **Electronic iris.** This is the first true method of digital signal enhancement that obviates the need for auto-iris lenses. Unlike its predecessors, the electronic iris works on true video signal averaging. This form of electronic enhancement literally de-amplifies the super-brights and amplifies the sub-blacks, creating an equal, 1 vpp video image. The result is that a person standing before a bright glass door is fully visible in detail, as are the surrounding features of the image. Manufacturers use a variety of names for the process.

- **Super Dynamics.**¹⁴ This analog method of electronic backlight compensation double-scans the CCD. The first scan is done at the standard 1/60 of a second, capturing images in the lower-light areas but washing out images in the bright areas. Simultaneously, the imager is scanned at 1/10,000 of a second, producing an image in the bright areas. Then the onboard processor combines the two images and the best of each is kept while the rest is discarded. The net result is a single image that has the best of both worlds. However, this technique does not work in all situations. In digital cameras, this method of image enhancement is referred to as multi-scanning

Cameras use various methods for handling difficult lighting situations, and manufacturers use different names for those methods. Few methods, however, are more effective than aiming the camera away from direct light. Eventually, obtaining good video in multiple lighting situations will be as simple as hanging a camera on the wall and aiming it correctly.

- **Auto focus.** This term refers to a camera's ability to focus on a scene automatically. While tracking an action or changing a scene, the camera and lens work in concert to focus the image. However, if the camera is pointed at something that is tucked into the middle of several objects that are closer, the electronics may have a problem determining what to focus on. Dome covers can also interfere with auto focus. For the most part, however, digital hybrids and auto focus IP cameras work well. The best equipment provides the option of turning auto focus off so the operator can focus manually in difficult situations.
- **Privacy blocking or image protection.** Through the addition of a specific control or a digital effect built into the camera, it is possible to obscure a specific area within an image. It only takes one liability case to realize that there are people behind the pan/tilts and zoom lenses. A few of the millions of CCTV cameras installed around the world stray from their intended uses and become invasive toys. Even in public settings, minor invasions of privacy can escalate into major problems, usually after captured images are made public.

Privacy blocking makes it possible to block specific elements of a scene, such as particular windows. Thanks to digital technology, the mask that is overlaid onto the image is mathematically attached to the relevant pixels, so the system works even when the camera pans, tilts, or zooms. This powerful feature is affordable and comes with various options, such as locked positioning or the ability to pan/tilt or zoom in or out while continuing to mask the desired area; flexible drawing or the ability to mask a section of the image regardless of its size or shape; blackout or

¹⁴ Super Dynamics is a trade name for a particular Panasonic technology.

focus tampering of the specified area; password protection against unauthorized reprogramming of the protected areas; and the ability to temporarily remove the mask or view through it during playback (after the fact) for valid purposes under controlled circumstances.

Other design factors. Designers must also consider the following:

- **Environment.** Does the camera need to be protected from vandals, customers, or employees? Must the camera housing blend in with existing decor? Interior camera housings are available in configurations ranging from ceiling mounts (designed to mount in place of ceiling tiles) to overhead bubbles to corner-mount stainless steel or bronze housings. Is the environment extremely dirty? Excessive dirt or dust buildup in the camera causes the unit to run hot and may limit its performance or life span. If the camera is to be mounted outside, other considerations arise. If winter temperatures in the locale drop below 35° F (1.7° C), the camera's protective housing will need a heater. Although CCD cameras can operate in cold temperatures, zoom and auto-iris lenses tend to slow down or freeze up because of the type of grease used in the iris, focus, and zoom rings. If summer temperatures rise above 80° F (26.7° C), the housing may need a fan or possibly an air conditioner.

If the unit will be installed in the sun, a sun shield will be needed to prevent excessive heat buildup in the camera housing. If the unit will face east or west, a sun visor may be needed to cut the glare from the rising or setting sun and to deter overheating. Often a sun shield can also act as a visor.

- **Mounting.** Mounting raises several considerations. If a camera will be mounted up high, how can it be reached for maintenance? Will the camera's angle of view be so steep that only the top or back of heads will be visible? Will the unit be mounted under an overhang, next to a wall, or above major obstacles such as air conditioning units? Will there be enough room to open the housing from the top, or will a bottom-hinged unit work better? Should the unit be mounted on a swing arm to allow easy access from a window or roof on upper floors? If the unit is to be mounted in a ceiling tile housing, is there enough room above the false ceiling to install the housing?

Another mounting consideration concerns what each camera is required to view and from what distance. For proper security viewing, one should not depend on the camera to view more than two objectives (one major and one minor), and the camera should not auto-pan (move side to side), either physically or digitally, more than 45 degrees left or right from the center of its major focus. Good video surveillance is often waylaid by expecting too much from a single unit or installing fewer cameras than are actually needed. The objective of the video system should be remembered at all times. With analog systems, the higher the security risk of the viewing area, the fewer objects each

camera should be required to watch. If using mega-pixel digital systems, a single camera can be used to watch as much area as two or possibly three analog cameras with the same quality or resolution of image. In high-security locations, it takes at least four analog cameras to view a 360° area, though the budget may force a compromise. With modern digital technology, there are megapixel 180° and 360° cameras that work with detailed software programs to promote multiple, individual or panoramic views.

STEP 5: CHOOSE THE PROPER LENS FOR EACH CAMERA.

This choice is determined by three different factors: camera format, distance from the camera to the scene, and field of view.

Format size. Format refers to the size of the imager area onto which the lens focuses light. That size is measured diagonally. The format size of the lens must match or exceed the format size of the camera. If the lens's format size is too small, the lens will not fill the imager with a picture, and the result will resemble tunnel vision. Thus, a 1/4 in. format camera requires a 1/4 in. format lens or larger (such as 1/2 in., 2/3 in., etc.).

Distance from camera to scene. This factor determines what focal length of lens is needed. The distance is measured from the front of the camera to the main subject being viewed. This distance must be measured accurately. If the camera will be mounted on the side of a building, 40 ft. from the ground, and the center of the scene is 30 ft. from the building, the relevant distance is not 30 ft. but 50 ft. The Pythagorean theorem shows that A^2 (the square of the distance from the side of the building to the center of the scene, or 30 ft. x 30 ft.) plus B^2 (the square of the mounting height, or 40 ft. x 40 ft.) must equal the square of the distance from the camera to the scene. This example results in an equation of $(30 \times 30) + (40 \times 40) = 2,500$, which equals 50^2 . Thus, the distance from the camera to the scene is 50 ft.

Field of view. The field of view (height or width of the area being viewed) determines the appropriate focal length for the lens. In the previous example, the distance from the camera to the center of the scene was 50 ft. Perhaps the desired scene is 20 ft. wide. With the use of simple math, a field-of-view calculator, a cheat sheet, or a view finder, it is possible to calculate the appropriate lens focal length. It is important to note, however, that the more area the camera views, the less detail it picks up. Working with megapixel technology, a larger area of view may be obtained without losing the required detail, or an equal area may be obtained with two or three times the detail of image. With megapixel technology, it is all about pixels per foot as opposed to being restricted to a fixed number of horizontal lines of pixel definition.

STEP 6: DETERMINE THE BEST METHOD FOR TRANSMITTING THE VIDEO SIGNAL FROM THE CAMERA TO THE MONITOR.

This step may be difficult for a typical security manager, who might prefer to leave it to the bidding contractor. Coaxial cable is generally sufficient for analog cameras but will not work for IP-based systems without the proper conversion electronics to transmit digitally encoded signals on coaxial. For distances of 1,000 ft. (305 m) or more between the camera and the control point, it may be best to use fiber-optic cable, regardless of the type of camera. Many transmission methods are available, and each has its advantages, disadvantages, and costs. Among those methods are coaxial cable, fiber-optic cable, twisted pair (two-wire) cable, Cat 5 or Cat 6 (networking) cable, microwave technology, radio frequency or other wireless technology, infrared transmission, and transmission over telephone lines, the Internet, or an intranet. A system might use more than one method of video transmission.

STEP 7: LAY OUT THE CONTROL AREA AND DETERMINE WHAT ENHANCEMENTS ARE NEEDED BASED ON EACH VISUAL ASSESSMENT POINT'S REQUIREMENTS.

Step 2 defined the purpose of each camera. With those definitions, the system designer can assign triggers and priorities and then determine which features the control equipment must have. For example, the designer might conclude that camera 1 requires digital video motion detection, an expandable pole, and an alarm interface; camera 2 requires a pan/tilt and zoom controller with pre-positioning; camera 3 requires alarm activation via a door contact; and the manager's office in building 5 needs access for viewing or controlling part or all of the system with password access.

Determining triggers and priorities for each camera helps automate the video system. It is inefficient and ineffective to assign people to sit and watch tens or hundreds of scenes continuously.

A recording or storage system is also needed. Such systems are available in many formats. For the most part, standard VHS and SVHS tape systems have fallen by the wayside in preference to digital recording. Digital recording or storage systems include simple DVRs (for use with analog-based cameras only), network video recorders (NVRs, for use with analog, IP, or hybrid cameras), and separate storage space located on a server or network or at off-site storage facilities via the Internet (cloud storage). The key to digital storage systems comes down to compatible formats between communicating cameras, compression factors, and required storage space on a per-image basis. It is all about math in the beginning and all about quality of the recalled image at the end.

5.6 EQUIPMENT SELECTION

This section discusses CCTV equipment in greater detail. The point is not to choose the equipment vendor but to define the operational parameters required by the application.

5.6.1 CAMERA

CCTV cameras come in four main types. Understanding the distinctions makes it possible to select the right camera for the task and avoid spending more money than necessary by buying unneeded features. The types are as follows:

- **Standard analog CCD cameras.** These may be black-and-white or color. The most common type of camera, these work well in all indoor and many outdoor applications. They are analog-based and may or may not have digital effects. Resolution ranges from 220 horizontal lines (very low) to 580 horizontal lines (very high). Light sensitivity varies between .005 lux (.00046 foot-candles), which is very low, to 10 lux (.929 foot-candles), which is very high. Color cameras are the most restricted by low-light situations. To compensate for that limitation, manufacturers have developed hybrid analog cameras. Some use infrared sensitivity to capture more light. Others combine color and black-and-white capability in one unit, capturing color images during daylight hours and black-and-white images at night when the light is low. Other cameras use an intensifier between the lens and the CCD to amplify the available light tens of thousands of times.
- **IP cameras.** These digital cameras come in black-and-white or color. Like their analog counterparts, IP cameras require visible light to create an image. These cameras are available in three basic styles: standard, megapixel, and smart. All IP cameras measure their resolution as a multiple of the Common Intermediate Format (CIF), which is a resolution of 352 x 240. This means 352 pixels on a horizontal basis with 240 pixels on a vertical. For all intents, CIF resolution is equal to about half the average 325 horizontal line analog resolution and so is not recommended as a usable standard for storage. Standard IP cameras range from one-quarter CIF (176 X 120) to four times CIF. 4 CIF means the user will have twice as many horizontal and twice as many vertical pixels to a single image or 704 x 480. Megapixel cameras range from 16 (1408 x 960) to 32 (2816 x 1920) times CIF or higher. Smart cameras can fall under either resolution range. They are called smart because they take advantage of their server base and employ computer programs within the cameras. Those programs enable the cameras to perform various functions, such as digital video motion detection, facial recognition, privacy blocking, digital pan/tilt and zoom, and more. They are often referred to as edge devices because they take the computing factors or features to the outer edge of the system as opposed to sending the information to the controller to be deciphered.

IP cameras may be powered via transformers or may be rated as “power over Ethernet” (POE), in which case they receive their operational power from the digital switching system via the network.

- **Infrared (IR) cameras.** These cameras require an IR light source to create an image. They are used where visible light is not an option.
- **Thermal cameras.** These require no visible or IR light to produce an image. Using special filters and lenses, the cameras monitor the temperatures of the objects in their field of view and use colors to represent temperatures. Cold objects are shown in varying shades of blue, while hot objects are shown in varying shades of red. Thermal cameras are often used in long-range surveillance, such as monitoring ships in a harbor five miles out. Since these cameras require no light to create an image, they are popular with police and border patrols.

5.6.2 LENSES

After choosing a camera, choosing a lens is the second most important decision of the project. The selection depends mainly on the size of the scene and the degree of visual identification required. Lenses come in five main types: wide angle, standard, telephoto, varifocal, and zoom:

- **Wide-angle lens.** A wide-angle lens captures a very wide scene and thus is best suited for short ranges—that is, 0 to 15 ft. (0 to 4.5 m).
- **Standard lens.** For an average scene at medium distance, a standard lens is needed. This type of lens reproduces a view equivalent to what the human eye sees at the same distance, except that the human eye has peripheral vision approximately two and one-half times that of a standard lens. A medium distance would be considered about 15 ft. to 50 ft. (4.5 m to 15.25 m).
- **Telephoto lens.** If the required view is a narrow area at long range, a telephoto lens is needed. A telephoto lens can best be compared to a telescope, as it enables the user to look at objects far away as if they are close. However, such magnification narrows the field of view. Long range is considered anything over 50 ft. (15.25 m).
- **Zoom lens.** A zoom lens incorporates moving optics that produce the same views provided by wide-angle, standard, and telephoto lenses, all in one device. These lenses may be manual or motorized. With a manual zoom lens, the installer manually adjusts the lens’s field of view and focus. Once set, the lens remains fixed. A motorized zoom lens has motors installed within the housing of the lens. This lens allows an operator, via a controller, to adjust the lens’s optic view from a remote location. The motorized

zoom lens also features a tracking mechanism, which is a physical tie between the focal optics and the zoom optics designed to automatically adjust the focus of the lens as the lens is zoomed out (from telephoto to wide angle).

- **Varifocal lens.** This is a smaller version of a manual zoom lens, offering the opportunity to tune the view on-site. These lenses enable installers to carry a few lenses in stock to cover a multitude of scene ranges. Varifocal lenses differ from zoom lenses in two ways:
 - They do not cover a full range from wide angle to telephoto but only a slight range on either side of a fixed focal-length standard lens (i.e., 8 mm to 12.5 mm).
 - They do not have a tracking mechanism and must be refocused each time their range is changed.

The next factor in choosing a lens is compatibility between the lens and the camera. Not only have cameras become smaller, but technology has changed lenses' ability to pass light; ability to reproduce a detailed image; size; electronic controls (now moved from the lens to the camera); and cost. Thus, lenses must meet several criteria to match a camera's physical and electronic needs. Incompatibility can cause physical damage and image problems. Over time, compatibility problems are being designed out of the industry, but meanwhile the following questions must be answered to determine a lens's compatibility with the application and the camera:

Question 1: Will the camera be installed in an area where the lighting is fixed, minimally variable, or highly variable?

This question determines whether the application requires a lens with a fixed iris, manual iris, or auto iris. As lighting has the greatest impact on performance, a fixed-iris or fixed-aperture lens has no adjustable physical control over the amount of light that passes through it. A manual-iris or manual-aperture lens can be opened or closed during installation to increase or decrease the amount of light that passes through it. An auto-iris lens uses a motor to open or close the iris. The need for more or less light is determined automatically by the video sampling circuit in the lens or camera.

Auto-iris lenses have become smaller, lighter, and less expensive than manual- or fixed-iris lenses. An auto-iris lens costs only a fraction of the price of a fixed- or manual-iris lens. In many applications, it is financially prudent to use auto-iris lenses on all cameras.

However, it may make sense to use a fixed- or manual-iris lens if the camera has a large light range, auto electronic shuttering, or an electronic iris. An auto-iris lens could conflict with the camera's electronics, causing extreme image flutter or total blackout.

Question 2: Is the camera a 1/4 in., 1/3 in., 1/2 in., 2/3 in., or 1 in., or megapixel format?

The format size of the lens must equal or exceed the format size of the camera. However, the format size of the lens has nothing to do with the final size of the image, which is determined by the focal length of the lens.

Question 3: Is the camera a color camera?

If so, a color-corrected lens must be used. A color-corrected lens has been ground differently and has a special coating on the optics of the lens. These measures ensure that the focal points of all colors in the visible light spectrum come to the same image focal point. Many older black-and-white cameras use noncorrected lenses. Therefore, reusing lenses may create problems.

Question 4: Is the camera a C or CS standard camera?

CS cameras were brought into production during the late 1990s. Their CCDs were moved 15 mm closer to the lens mount, so CS lenses do not penetrate as deeply into the camera. However, many cameras meeting the older C standard are still in use, and lenses meeting the C standard are still being sold. Thus, it is important to check whether the camera accepts C or CS lenses. Mounting a C lens onto a CS camera without an adapter ring will crack the CCD. However, with an adapter ring, the image and camera will be fine. Mounting a CS lens on a C camera causes incurable focus problems. Some cameras can work with both C and CS lenses.

Question 5: Will the camera accept an AC/EC (video) or DC/LC lens?

AC stands for auto circuit, and EC (electronic circuit) is its metric equivalent. DC stands for direct circuit, and LC (logic control) is its metric equivalent. For the most part, the DC/LC lens has become the standard for camera and lens design.

The AC/EC (also called video) lens uses the original, antiquated auto-iris lens design. It has a video sampler circuit built into its body to control the iris based on the video signal level of the camera. To cut the cost and increase the efficiency of auto-iris lenses, the DC/LC was developed. This lens has no electronics built into it for iris control but rather depends on the camera to supply it with the necessary positive or negative motor voltages to operate the iris.

Older cameras accept and operate video lenses but not DC/LC lenses. Most cameras designed after 1995 and before 2002 accept either the video or DC/LC lens. Cameras designed since 2002 accept only the DC/LC lens.

Question 6: Is the camera a megapixel camera?

The primary difference between a standard lens (of any format as listed above) and a megapixel lens is that the megapixel lens is considered to be a much higher quality lens. All

lenses are designed to focus or define the viewed image on a pixel by pixel basis. For example, with a 4 CIF camera and lens, the lens is designed to focus on an area equivalent to the size of a single pixel point. If the 4 CIF lens is mounted on a 16 CIF (1.3 megapixel camera), the primary difference is that there will be twice as many horizontal and vertical pixels installed on the 16 CIF CCD, which means they are also half as large in surface area. This also means the 1.3 megapixel camera has two vertical and two horizontal pixels (four pixels total) in the same space as the 4 CIF camera has one. Therefore, the 4 CIF lens on a 1.3 megapixel camera would focus the image on four pixels as opposed to one, causing the overall image to be equal to 4 CIF. The result is wasted technology, money, and effort.

Question 7: Does the application use infrared (IR) enhancement lighting?

If so, the camera should use an IR-corrected lens. Like a color-corrected lens, an IR-corrected lens uses special optics and coatings to ensure that the longer IR light waves are focused on the CCD.

In the end, compatibility problems between cameras and lenses can be avoided through careful attention to camera and lens specification sheets. Camera specification sheets tell which lenses the camera will accept. Lens specification sheets tell whether the lens will live up to the demands of the camera. It is not essential to understand all the processes that make a piece of equipment work. However, it is essential to understand the basic principles and nomenclature.

5.7 **CAMERA FORMATS AND LENSES**

As CCDs shrink, it becomes increasingly difficult to match lenses with cameras. For instance, a site might have 1/4 in. cameras with 6.5 mm–65mm zoom lenses. If the security manager wants to add a 1/3 in. camera to the site, he or she must determine what lens on the 1/3 in. camera will provide the same view. The key is to know what the standard lens for a camera is and then calculate from there. A 25 mm lens is the standard lens for a 1 in. camera. (A standard lens recreates an image equivalent to what the human eye sees at the same distance.)

A 1/2 in. format CCD is half the size of a 1 in. format CCD. Therefore, the standard lens for a 1/2 in. camera should be 12.5 mm—half the size of the standard lens for a 1 in. camera. Likewise, the standard lens for a 1/3 in. camera is one-third of the 1 in. standard, or 8.333, rounded to 8mm.

It is a little more difficult to determine the right lens if a 1/2 in. camera in the field, using an 8 mm lens, will be upgraded to a 1/3 in. format, and the same image size is desired. The first step is to convert the 1/2 in. camera and lens into equivalent terms for a 1 in. format camera and lens. A 1 in. camera is twice the size of the 1/2 in. camera, so the 1 in. camera's lens would be twice the size, too. The 8 mm lens thus equates to a 16 mm lens on a 1 in. camera. The next step is to convert the 1 in. equivalents into a 1/3 in. format equivalent. Thus, 16 mm divided by three equals 5.33 mm. In this case, the best choice might be a 1/3 in. varifocal lens with a range that includes 5.33 mm. An alternative would be to select a lens with a fixed focal length close to 5.33 mm, in a 1/3 in. format or larger.

The field of view is the final size of the viewing area as measured in width and height. Analog systems create rectangular images that are four parts wide by three parts high. If an image is 12 ft. wide, it must be 9 ft. high. The field of view for IP or digital cameras works in much the same manner except that the image is no longer fixed at 4 x 3.

Resolution of digital cameras is measured in terms of the Common Intermediate Format (CIF). The resolution ratings of all digital cameras are multiples or divisions of CIF. The most common IP resolutions (to date) are as follows:

| Ratio | Label | Horizontal x Vertical Array | Grid |
|-----------------|--------|-----------------------------|-----------------|
| CIF | CIF | 352 x 240 pixels | 84,480 pixels |
| Quarters of CIF | Q CIF | 176 x 120 pixels | 21,120 pixels |
| 4 times CIF | 4 CIF | 704 x 480 pixels | 337,920 pixels |
| 16 times CIF | 16 CIF | 1,280 x 1,024 pixels | 1.31 megapixels |
| 25 times CIF | 25 CIF | 1,700 x 1,200 pixels | 2.04 megapixels |
| 36 times CIF | 36 CIF | 2,112 x 1,440 pixels | 3.04 megapixels |

A 4 megapixel image has the same resolution as 400 ASA film. A 6 megapixel digital image has the resolution of 100 ASA film.

The resolution of an image is determined first by the camera, second by the transmission method, third by the weakest link in the video system interface, and fourth by the reproduction capability of the image storage system. The higher the resolution, the sharper the image.

High-resolution cameras produce low-resolution images if low-resolution monitors or high compression algorithms are used. The monitor, however, is seldom the problem. Analog video recorders average a playback of 325 horizontal lines. Thus, the camera's high-resolution

image may look good on the monitor but poor when a recording is played back. Multiplexers are another source of loss. These units take the video signal in, digitize it for features and switching, and then turn it back to analog, losing up to 25 percent of the resolution in the process. Moreover, coaxial cable can cost another 10 percent to 15 percent of resolution due to sloppy installation, bad connections, and cheap cable.

Digital resolution, by contrast, is ultimately unlimited and extremely flexible. A digital image can be made smaller in both bandwidth and storage requirements through compression algorithms. The most effective and fastest growing compression standard in the digital imaging market is H.264. This algorithm allows for good compression with little or no effective loss of detail. The key to remember is that once an image is compressed, it very seldom is able to be returned to original quality or detail.

Resolution is not a major issue in most indoor applications and many outdoor applications. Still, if a security manager must rely on recorded images for information, he or she should ensure that the object of interest is large enough to be identified clearly or that after compression, there are enough pixels per foot (or meter) to insure accurate recognition according to the requirements of the original intent of the system design.

5.8 **CONTROLLING SOFTWARE**

Most modern systems today are either tied directly to a DVR (analog), NVR, or server. In the case of DVR or NVR systems, all controls, features, or benefits are part of the units that are used together. For larger, more complex applications, all the video information will be gathered on a network and controlled at a central point via software applications. Again, depending on the size of the final system, the software required by the system may be simple enough to operate from a single personal computer. For larger, more complex applications, the entire software package may require extreme computing power and equal software. Care should be taken to answer key questions required for a good system or application design:

- **How many cameras will be handled at each node point?** With digital systems, because of restrictions in cable length and access, most cameras will be cabled to the nearest node as opposed to being on a “home run” to the central control point. Again, this will be determined by the overall size of the area of installation. A node is a central point for individual pieces to come together for insertion onto a network path. The network path is just what it sounds like: a central connection between all field nodes and the head-end. Consideration must be given to how much equipment will be connected at each node point to ensure that appropriate encoding, power, and switching equipment is

installed along with the amount of bandwidth that each node will ultimately use while communicating with the head-end.

- **Will any of the cameras be viewed at more than one monitor point? If so, will the individual monitor points need separate controlling capabilities?**¹⁵ The purpose of this question is to determine cabling requirements, individual bandwidth requirements for transmitted or received data, and the capabilities or requirements of the software base that drives the system.
- **Will there be any interfaced alarm trigger points?** As a video system grows, it may become advantageous to install alarming devices (such as door contacts, infrared motion detectors, and photo beams) to trigger a single camera onto the screen when an intruder or motion is detected in an area. An advantage is that the operator can concentrate on other tasks until the alarm is triggered. Smart or edge cameras often offer alarm inputs at the camera. This avoids the need for additional cabling from the alarm contact to the nearest node or head-end.
- **Will the switcher be required to trip any other devices, such as buzzers or lights, in the event of an alarm? Would it be advantageous to transmit an email, text, or video image to a portable device, such as a mobile phone?**
- **Are there plans to expand the system in the future? If so, can the network and individual nodes handle the expansion?** If a node is installed with 16 inputs and a small power supply in a wall-mounted box and there are plans to add six or seven cameras down the line, it may become necessary to replace the power supply, switching system, or lock box when the time comes—unless the designer left enough room and chose the right size of equipment up front. Planning ahead could mean the difference of hundreds or thousands of dollars when the time comes to expand.
- **What units will need to be rack-mounted? Is it better to use a table or desktop application?** The answer influences some ancillary decisions in the selection of the type of monitoring station.

The final layout of the nodes, head-end, and all associated switching, encoding, network, and software cannot be done until the initial cameras views are fully decided.

¹⁵ Controlling capabilities include the ability to pull up individual pictures or control lenses or pan/tilt units.

5.9 RECORDING SYSTEMS

When it comes to retaining and using images of security events, the user must decide whether the system's purpose is to verify information, prove it, or aid a prosecution with it. This decision leads to the type of video imaging, degree of quality or resolution, and number of images per second/per camera that are best for the situation. For example, if the video information is to be used in the courtroom, its admissibility may be determined by the quality of the recorded information, the way it was obtained, and proof of originality. It makes sense to check with the organization's legal team before installing the system. Other than that, modern storage systems come down to a simple formula of how many images at what resolution may be stored over how much time.

For example, if a single 1.3 megapixel, H2.64-format camera is providing 15 images per second at a storage rate of 2.35 Mb per image, one needs 35.25 Mb of storage space per second, for this single camera. That is an unrealistic amount to store. To save space, once can reduce the number of images per second, the amount of resolution required (usually via compression factors), the actual amount of recording time per unit (via triggers such as video motion detection), and more. It may be useful to meet with the manufacturer of a server or NVR system to calculate storage requirements based on final design requirements. At the end of the day, the only reason to cut down on the amount of bandwidth requirements of the network and the amount of storage space required is cost.

The following are the basic types of recorders:

- **Digital video recorders (DVRs) (analog).** DVRs capture analog signals and convert them to digital formats. These recorders store video data on a hard drive, CD, DVD, or other medium. The challenge is that the video data requires a great deal of storage space. Therefore, DVRs compress the video image, using a particular codec (a compression engine or command sequence that causes the unit to combine colors, drop resolution, or both). Once compressed, however, the image quality may be poor. It is important to test DVRs (playback and enlargement features in particular) before purchase.
- **Network video recorders (NVR) (digital).** NVRs are designed to accept either digital or analog signals from the field. They are much better than DVRs and are similarly designed to be controllable over a network. These units also come with a high degree of sophistication and are usually adequate for systems with several hundred cameras. Although most NVRs have good search techniques, they are often limited in the amount of interfacing or features available to outside applications, such as access control or alarm system. Additionally, most NVR systems are not accessible to outside software solutions that may be required by the overall security and response design.

- **Server/cloud applications (digital).** For systems that require sophisticated software applications for control, analytics, or other intricate interfacing, and for very large systems, storage usually consists of compressing the incoming digital signals and storing them in complex levels on servers. These systems offer sophisticated search methods as well as multiple visual outputs for delivery to both fixed and mobile applications. These software systems can offer everything from variable frame rate on a camera-by-camera basis to complete digital control for zooming and pan/tilt functions.

5.10 ADDITIONAL DESIGN CONSIDERATIONS FOR VIDEO ASSESSMENT

A video assessment system should be designed as a component of the total intrusion detection system. Many interactions between the video system, intrusion sensors, and display system should be considered during conceptual design, such as these:

- site/sector layout—layout of sensors so that assessment is possible at a reasonable cost
- video/sensor interference—design of the assessment system to avoid contributing to the cause of sensor nuisance alarms
- monitor location—location of video monitors in the display system
- construction—common construction and installation requirements, techniques, and locations

Site/Sector Layout

One requirement of a perimeter assessment system is to display as much as possible of the clear zone, including both the inner and outer fences. Camera/lens selection and positioning must ensure detection and classification of any visible cause of fence and sensor alarms for the clear zone at any time. For these reasons, it is important that the following criteria be observed: (a) the inner/outer fence spacing should be relatively uniform; (b) minimum width restrictions for the clear zone should be considered; (c) grading or removal of vegetation of the clear zone should be performed; and (d) adequate area illumination must be provided. Changes from these criteria will generally reduce system efficiency and increase overall system cost by increasing the camera and equipment requirements to achieve an acceptable level of system effectiveness. Each exterior assessment zone should use one fixed camera per zone to provide assessment capability.

The effect of using more than one camera to assess a single alarm on interior locations should be considered. At smaller or lower threat facilities, with only a few cameras or with particular video coverage requirements, multiple cameras per alarm may provide acceptable assessment without an undue duplication of display and recording equipment. Large systems tend to be simpler if each alarm is assessed by only one camera, since decisions regarding which cameras are to be switched will be simpler and the operator will be able to concentrate on a limited selection of video for review.

Video/Sensor Interference

Typical exterior systems require installation of camera towers near the area where sensors are installed. Tower height and location must be chosen so that pole vibration caused by wind does not create a source of seismic energy sufficient to cause buried cables to alarm. In addition, camera towers should be placed to prevent their use by an adversary in crossing the perimeter or isolation zone. Power, video, sync, and control lines must be placed where noise cannot be induced between video cables and sensor cables.

Monitor Location

Video monitors should be installed in the system control console in a location that allows effective, rapid assessment without interference from other system controls and outputs.

Construction

Installing signal and power distribution cables and modifying buildings for equipment installation will be common for many parts of an intrusion detection system. Decreased construction costs and more effective system design will result from combining sensor subsystem and assessment subsystem requirements, such as conduit and junction box installation. Room for system expansion should be included within these construction elements.

Alarm Assessment by Response Force

Video alarm assessment can be complemented by visual checks from security officers. If the video assessment system is not operable (maintenance, weather) or if video assessment is not available for a particular situation (for example, use within some classified facilities), security officers must be able to assess the alarm.

Regardless of whether alarms are assessed using video or security officers, the alarm must be assessed quickly after it is reported to be most effective. For facilities that use towers, security officers in towers can provide effective assessment if the number, design, and placement of the towers are adequate to provide complete visual coverage of the perimeter. Patrols or roving officers sent to investigate an alarm can provide effective assessment only if they are

able to respond in a timely manner (i.e., before the intruder or nuisance source disappears) and there is still ample delay in the system.

Integration with Safety Systems

Today it is common to add many CCTV cameras to a facility to help in determining the presence of a safety-critical event. While these measures may reduce labor costs, there may also be a decrease in security system effectiveness. In large or complex facilities, it may be better to separate these functions so the security force will not be distracted by safety events, which could mask a malevolent attack on the facility. In simple facilities with low-level threats, co-location of these functions may be acceptable; however, this may still compromise security system effectiveness during an attack.

Legal Issues

Proper attention to privacy is a major consideration when using CCTV systems. It is generally inappropriate to locate cameras in locker rooms, bathrooms, or other places where employees or visitors have a reasonable expectation of privacy. Use of hidden or covert cameras is legal under many circumstances, but consultation with an attorney is recommended to be sure that enough justification or legal authority exist for this use. It is also a liability to use dummy cameras at a facility. Doing so establishes an expectation of protection, which can create a liability if a person is under attack and believes that the attack has been noted and help is on the way. It is also an accepted legal practice to post signs informing people that an area is under video monitoring or surveillance. These signs are often placed at facility entry points to minimize the number of signs and to alert visitors and site personnel of the presence of CCTV.

The use of recorded video information must meet certain standards to be admissible as legal evidence. Depending on the jurisdiction, quality of image, time/date stamp, and percentage of scene occupied by the subject, an eyewitness may be required. In addition, in many states the presence of a unique scene identifier is also required. This identifier serves to conclusively establish where the image was recorded. For example, it is necessary to differentiate one office or hallway from another. Electronic images are now using digital watermarks to ensure image integrity and eliminate tampering but have achieved varying levels of legal acceptance. To be certain that recorded images will meet legal requirements, consultation with an attorney or law enforcement agency in the jurisdiction is recommended.

Procedures

Camera selection should be based primarily on the sensitivity required for a full video output signal in the lighting environment in the area to be assessed. The sensitivity must match the lighting design goals, regardless of the imager. The resolution of the imager is next in importance because it determines the number of cameras required for a given straight-line

perimeter selection. The greater the resolution, the greater the spacing between the cameras can be. The object resolution required should be determined before the camera selection, but in practice the desired object resolution may be slightly modified when the possible camera choices are limited.

Camera format is an important consideration in the camera selection process. The format size determines the sensitivity of the image tube, with smaller formats having reduced sensitivity as well as lower resolution. The trade-off in this situation is price, but the cost of the camera is only part of total system cost. Format size also affects the field of view, which dictates the number of lenses available in a variety of focal lengths. The requirements of specially designed lenses for nonstandard focal lengths should be considered and evaluated carefully.

During the selection process, evaluation of cameras should be undertaken under the real lighting environment expected at the site. In many cases, the experience of other facilities can help to reduce the number of options considered. Manufacturers' literature should not be the sole criterion in camera selection. The specifications, or the conditions under which specifications are developed, may be unrealistic in relation to the design problem at hand.

Other considerations in the selection process should include the difficulty of maintenance, the packaging of the camera for the environment in which it will be used, maintenance support from the manufacturer, and documentation supporting the equipment. Documentation should include operating, adjustment, and maintenance procedures; theory of operation; block diagrams; schematics; and manufacturer and commercial replacement parts lists. Serious consideration should be given to eliminating any product that does not include such documentation.

Acceptance Testing

A video assessment subsystem requires a conscientious approach to installation and maintenance to ensure maximum performance. An incoming inspection should be made of any cameras purchased for evaluation or for final system installation. Different parameters will be evaluated for the two situations. Evaluation cameras will be compared to other cameras purchased for the same purpose. Upon receiving cameras for the final installation, camera performance should be evaluated to determine conformity with the manufacturers' specifications, compatibility with the design criteria, and consistent performance from camera to camera. Experience has shown that final inspection at the manufacturers' plant is not consistent, and performance may deviate considerably from the specifications. Frequently some equipment has been damaged or had parts shaken loose in transit. Operating the equipment continuously for a few hundred hours before final installation usually decreases the maintenance problems during the installation phase of perimeter construction. Any

problems discovered at this point should be referred to the manufacturer for resolution while still under warranty.

Exterior cameras should be installed according to manufacturer specifications and focused at night under the same type of lighting expected in normal operation. If possible, cameras should be evaluated for their resolution capabilities prior to purchase. One simple method of checking for camera resolution is to use appropriately sized targets in the assessment zones and verify that they can be classified. For example, one can use targets shaped as a 1 ft. (0.3 m) diameter circle, a 1 ft. square, and a 1 ft.-high triangle. The targets are painted black on one side and white on the other. By placing the targets at the far field of an exterior perimeter assessment zone and having an operator view the image and recognize each of the distinct shapes (classify), one can rapidly determine whether system resolution is adequate. The targets can also be moved to bright and dark areas to verify that the images are still identifiable (using the appropriately colored side of the target—black for dark spots, white for bright spots). The size of the target can be varied depending on the expected threat at a facility, or resolution charts can be used to determine resolution in interior or exterior assessment zones. One-foot targets simulate the cross-section of a crawling person; larger or smaller targets may be more useful at other facilities, based on the threat. Additional aids in determining resolution include the use of a large resolution chart in the assessment zone or the use of test targets made by CCTV manufacturers, such as a Rotakin. Due to the lack of accepted resolution standards or requirements for private security system integrators, the system designer or security manager should determine what resolution is needed and specify this when placing contracts or buying equipment.

Camera performance can also be verified in a laboratory using a test bench. This allows measurement of resolution, focus, and sensitivity and can be more cost-effective than performance testing. The initial verification of camera performance using a test bench is not sufficient to ensure acceptable performance in a protection system. Some CCTV cameras are shipped prefocused; however, the environment that these cameras are focused in may not be the same as the operating environment at a facility. Initial testing and verification should be followed with appropriate indoor or outdoor testing to confirm that cameras perform as required. Final adjustments to camera focus, sensitivity, and field of view to account for actual lighting or other environmental conditions can be performed at this time.

Exterior lighting surveys should be performed using high-quality light meters and a grid pattern—for example at 3 ft. (0.9 m) intervals, 1 ft. (0.3 m) above the ground. A survey should be conducted at lighting installation and then repeated yearly thereafter. A preventive maintenance schedule for light replacement should be prepared. Depending on the size of the facility and the available budget, all lamps can be replaced at the same time or lamps can be replaced as they fail. In many cases, lamp replacement in exterior areas requires a bucket truck or similar equipment. If such equipment is permanently available at the site, there is

greater latitude in the maintenance schedule than if the equipment must be rented. This equipment can also be used in the replacement or maintenance of exterior cameras. Over time, enough data can be collected to establish a routine replacement cycle for lamps. In addition, lighting initiation is important. A variety of approaches exist, such as using one photosensor to activate all lights; one cell per light, per side, or per sector; or manual activation.

Interior lighting should also be evaluated on a continuing basis but will not require as substantial an effort as exterior assessment areas. Specifications exist for the amount of light that should be present to enable various tasks, such as reading, inspections, or general office work. In most indoor applications, the lighting provided to illuminate the work being performed is also adequate for CCTV cameras; however, this should still be verified. Particular attention should be paid to moving furniture or other objects in internal assessment areas to eliminate shadows or blind spots.

The speed of the video subsystem should also be tested to be sure that alarm sensing and video capture happen rapidly enough to capture the actual intrusion event. Performance tests on the number of alarms that can be captured and reported within one second, camera switching times, and recording times can also help determine if the system is performing as expected. In addition to performance tests on the video subsystem and its components, use of acceptance tests for any video subsystem provided by a vendor or systems integrator is strongly encouraged. These tests should address the adequacy of resolution under actual operating environments, speed of recording, number of alarms that can be acquired and stored for review in one second, and related details, such as light-to-dark ratio. The desired specifications and statement of acceptance testing should be included as part of the terms and conditions in contracts with vendors.

With incoming inspection and equipment burn-in prior to installation, maintenance problems should be minimized for the short term. Camera adjustment will probably consume most of the maintenance time. Optical focus of the camera lens has consistently been a major, time-consuming factor in original installation. Day-to-night illumination levels and energy spectrum changes are responsible for most of these problems. Optical focus is more reliable if accomplished at night under the appropriate scene lighting from the final camera location. Cameras in sealed environmental housings typically pose a serious restriction to this procedure.

Maintenance problems are best resolved by a competent, on-site staff capable of understanding the complexities and interrelationships of all the concepts used in the original system design, as well as having a background in electronic systems troubleshooting. Specific, periodic maintenance requirements should come from the equipment manufacturer in the form of printed documentation. Also, it is useful to have a specification for nuisance alarm

rates, as this will allow some number of nuisance alarms to occur without penalty. The value of occasional nuisance alarms is that they maintain confidence that the system is working. An example of a nuisance alarm specification might be one nuisance alarm per zone per day. The number should be small enough to allow continuing operation under expected varying conditions, but not so high that a vulnerability is created. This can occur if there are so many nuisance alarms that security officers are tempted to ignore them. Any recurring nuisance or false alarms should be investigated for possible system improvement. As with any security equipment maintenance performed by outside personnel, all equipment should be checked after the maintenance activity to ensure that systems are fully operational and unmodified.

Equipment logs should be kept that detail replacement or repair of various system components, and appropriate spares should be kept on hand. Depending on the budget and site size, 10-20 percent spares are recommended, especially for cameras. If cameras are replaced by newer models or different types, they should be tested for compatibility and performance and appropriate notes made in the maintenance log. Contingency plans must be developed to explain what will be done if CCTV capability is lost for varying periods of time or at one or more locations. Options may include assigning a guard to the location until the system is repaired or deploying portable systems.

Manufacturers' equipment documentation should be preserved at the using site as well as at a central document storage location. Any equipment modifications made on-site should also be documented and stored at these two locations. A maintenance log of all camera repairs and adjustments should be kept to provide a historical record of each piece of equipment. Maintenance trends can be established to identify recurring problems and equipment failures. This practice will substantially reduce repair time and identify any equipment performing in a substandard manner.

5.11 **EVALUATION OF VIDEO ASSESSMENT SYSTEMS**

The following parameters determine the effectiveness of a video assessment subsystem:

- minimum time between sensor alarm and video display
- complete video coverage of the sensor detection zone (called the assessment zone when sensors and video are integrated)
- ability to classify a 1 ft. (0.3 m) target at the far edge of the assessment zone (Classification means an object in the video image can be accurately differentiated as human, animal, blowing debris, or other category. Some protection systems must identify the object in the image; identification is the ability to differentiate between people, for example, John not Jim. These capabilities are a function of image quality, which is measured using video resolution.)
- vertical field of view at far edge of exterior detection zone to account for the height of a standard fence (if present) and a person climbing over the top of the fence
- continuous operation, 24/7
- minimal sensitivity to environmental conditions for all cameras
- minimal obscuration of the assessment zone (such as trees, fences, or junction boxes in exterior areas or furniture that blocks the camera view in interior areas)
- camera field of view and video recording system integration that displays the alarm source to an operator

The more the assessment subsystem deviates from these requirements, the lower the quality of the video image and the more subsystem performance will be degraded.

Evaluation of video surveillance systems generally verifies that cameras and pan/tilt/zoom controllers are operational and that time/date stamps or other text messages are accurate.

To support testing of the video subsystem, test targets can be used to verify video image quality. These targets are simple geometric shapes that include a 1 ft. (0.3 m) diameter circle, a 1 ft. square, and a 1 ft.-high triangle. The test target sizes are based on a horizontal field of view of six horizontal television lines (HTVL) per foot as the required resolution, which is sufficient to classify a crawling intruder under appropriate lighting. If the expected threat will always provide a larger profile to the video system, a lower horizontal resolution is acceptable. Using the test targets is appropriate in both cases. The test targets are painted black on one side and white on the other so they can be used to check image resolution in dark and bright spots, respectively. Because the evaluation must consider component performance under a variety of changing conditions, this is a simple way to test whether the

test targets can be seen at lighting extremes in the area. These targets are used for testing both black-and-white and color cameras.

The targets are placed at various points in assessment zones (or across the camera field of view, if using a surveillance system), and the subsystem operator is asked to distinguish the different targets. The more targets that can be clearly differentiated, the more confidence one can have in the quality of the video image. Locations selected for testing are those that do not appear to make target identification easy, such as dark or bright spots or places where the camera view is obstructed or where the surface may not be level. The tests can be performed for both exterior and interior cameras. These targets test the extremes of the black and white capabilities of the assessment subsystem against the background color the assessment zone. Other aspects of video image quality that must be considered are lighting, camera mounting, the transmission system used, and the integration of switchers and controllers into the subsystem to facilitate alarm assessment.

The test targets are also used to check far-field resolution, particularly in exterior assessment zones. Because the far field represents the furthest distance from the camera, it will have the fewest lines per foot, so this is a quick way to verify that the horizontal resolution is maintained across the entire assessment zone.

Quality of the live video image is just one aspect of the evaluation. Because it is unlikely that all alarms can be assessed using live video (think of multiple alarms, operator attention to other tasks when an alarm is initiated, or an adversary running very fast through a detection zone), a video recording and storage system is also needed. As with cameras, there are many choices to accomplish this, but what is important is that the recording and playback happens fast enough and with enough detail to determine the cause of the alarm. Speed of playback and display is less important when the response will be after-the-fact review, as long as the image quality is sufficient to assess the alarm. The video test targets can be used to verify image quality for recorded images. It is likely that the recorded image will not have the same resolution (i.e., quality) as the live image, but that varies with different recording media and settings.

The test targets may also be used to test video surveillance systems. In this case, video image quality can be tested, although these systems depend on human operators to actually see a security event occurring in a live view, or assume that a delayed response using recording is all that is needed. If this approach will work for the facility, the test may be appropriate. In addition, many video surveillance systems use pan-tilt-zoom (PTZ) cameras and so may not be viewing an area of suspicious activity.

5.12 **WHERE CCTV IS HEADING**

CCTV is heading toward being completely obsolete as it is fully replaced by DIS (digital imaging systems). Functions and features continue to expand as the capabilities of the overall system design continue to become more automated. With digital control and storage systems already, it will be only a few years before the availability of fully automated, intelligent systems. Those systems, once programmed, will not require manual monitoring of any sort. Such systems will include full facial recognition on an average system as well as point-to-point, system-to-system (citywide) tracking of individuals or groups.

CHAPTER 6

LIGHTING

The study of lighting involves many disciplines: lighting science and technology, electrical systems, aesthetic design of fixtures and socioeconomic considerations, such as cost, light trespass, and the effect chemicals (such as mercury used in lamps) have on our ecology. In contrast to the technological nature of lighting, the application of lighting to real-life scenarios, in particular for security and safety, requires an appreciation of the subjective reaction of people to different lighting environments. Artificial lighting has developed almost exclusively for the benefit of humans so they may continue to perform occupations, sports, leisure activities, and any other life activity in the absence of sunlight.

Security lighting serves three primary functions—it can act as a deterrent to criminal activity, it provides life-safety functions (such as lighting pathways and parking lots), and it lights an area for the use of video subsystems. However, lighting comes in many forms. Some are more effective than others, and some are more expensive than others. This chapter provides a basic understanding of lighting science and its terminology, the features and benefits of different types of lamps, and the effective application of lighting to increase safety and security in the work environment.

6.1 LIGHTING AND LIGHTING DEFINITIONS

The quantity of light emitted by a lamp is measured in lumens. For example, a typical household bulb rated at 100 watts might output about 1700 lumens. A spotlight and a floodlight might output the same quantity of light, but the spotlight concentrates its output in a small area, whereas the floodlight disperses the light over a larger area. Illuminance is the concentration of light over a particular area. Illuminance is measured in lux, representing the number of lumens per square meter or in foot-candles (fc), the number of lumens per square foot. One footcandle is equal to 10.76 lux (often approximated to a ratio of 1:10).

The sensitivity of a CCTV camera can be defined as the minimum amount of illumination required to produce a specified output signal. The following factors are involved in producing a TV signal:

- illuminance level of the scene
- spectral distribution of the illumination source
- object reflectance
- total scene reflectance
- camera lens aperture
- camera lens transmittance
- spectral response of the camera imager
- video amplifier gain, bandwidth, and signal-to-noise ratio
- electronic processing circuitry

Camera sensitivity is usually specified as the minimum illuminance level that will produce a full 1 volt peak-to-peak video signal. The specification should state whether the indicated illuminance level is the scene illuminance or the faceplate illuminance. The illumination source is usually an incandescent lamp operating at a color temperature of 2,854° K. In some cases, the parameters used to claim this sensitivity are unrealistic. Two of the favored parameters are higher scene reflectances than are normally encountered and greater transmittance than is commonly available in standard auto-iris lenses with neutral density spot filters.

Figure 6-1 provides a measure of light levels from common experience.

The amount of light necessary to produce a usable video signal from any video camera is a function of these factors:

- the type and brightness of the source
- the amount of light energy illuminating the scene of interest
- the portion of the light reflected from the scene
- the amount of light transmitted by the lens to the imager
- the sensitivity of the imaging device itself

An understanding of the relative levels of scene illumination produced by natural sources, the amount of light reflected from typical scenes, and the resultant faceplate illumination levels required by the variety of image tube and solid-state imagers is important to the successful deployment of even the simplest CCTV system.

| Light Level (footcandles) | Natural Light Source | Visual Experience Light Levels |
|------------------------------|----------------------|----------------------------------------|
| 50,000 | | Upper limit of visual tolerance |
| 10,000 | Direct sunlight | Fresh snow on a clear day |
| 1,000 | Full daylight | Average earth on a clear day |
| 100 | Overcast day | Average earth on a cloudy day |
| 1 | Twilight | White paper 1 ft. from standard candle |
| 0.1 | Deep twilight | |
| 0.05 | | Snow in full moon |
| 0.01 | Full moon | |
| 0.005 | | Average earth in full moon |
| 0.001 | Quarter moon | |
| 0.00005 | | Grass in starlight |
| 0.00001 | Overcast night | |
| 0.000001 | | Absolute limit of seeing |

FIGURE 6-1
Natural and Visual Light Levels

The percentage of light reflected from a scene (reflectance) depends on the incident light angle and on the texture and composition of the reflecting surface. For natural illumination, the reflectance of various scenes is relatively independent of the angles of incidence and reflection. Figure 6-2 lists some common surfaces and their approximate reflectances (McGhee & Pierce, 1990).

The two most important parameters of a lighting system for CCTV are its minimum intensity and its evenness of illumination. The intensity must be great enough to ensure adequate performance of the chosen camera system. A minimum of 1.5 fc is required for a camera system using an f/1.8 or faster lens and a solid-state imager (Greenwoll, 1991). This assumes a ground surface reflectivity of 25 percent. Of equal importance is the evenness of illumination, which is characterized by the light-to-dark ratio (maximum intensity to minimum intensity). An excessive light-to-dark ratio will produce unacceptable pictures in which the bright areas appear washed out and the darker areas appear black. A design ratio of 4:1 is preferred to allow for environmental and other degradation factors to achieve a 6:1 maximum over time.

| Material | Reflectance |
|----------------|-------------|
| Asphalt | 5% |
| Concrete (old) | 40% |
| Concrete (new) | 25% |
| Red Brick | 25% |
| Grass | 40% |
| Snow | 95% |

Figure 6-2
Reflectance Measurements

Cameras are light-averaging devices, so when deploying them it is necessary to ensure that the light level in the camera’s entire field of view is illuminated evenly, not only the assessment area. Light contours are distributed throughout the field of view, and the entire field of view contributes to the light-to-dark ratio, not just the area between the fences. Computer programs that model the expected light level from a variety of lamps can be used to assist in the initial design and layout of exterior and interior lighting. These results should be validated by measuring actual light levels in an area with conditions similar to those expected in the application. After implementation of the final lighting design, lighting surveys should be performed to establish a baseline light-to-dark ratio and periodically thereafter to establish the proper maintenance and replacement schedule.

Corrected color temperature (CCT) is a measure of the warmth or coolness of a light. It is measured in degrees Kelvin, which is the centigrade (Celsius) absolute temperature scale where 0° K is approximately -272° C. To grasp the concept of color temperature, it helps to think of a piece of metal being heated in a furnace. When it starts to glow red hot it is about 2700° K, white hot is about 4100° K, and blue hot is about 5000° K—similar to daylight. People often perceive red hot as being warm and white or blue hot as being cool.

The color temperature of a light source has a considerable impact on mood and the ambiance of the surroundings. Figure 6-3 summarizes the color temperatures of various types of lamps and their applications (Phillips Lighting Company, 1999).

| Color Temperature | Warm 3000° K | Neutral 3500° K | Cool 4100° K | Daylight 5000° K |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Associated effects and moods | Friendly Intimate Personal Exclusive | Friendly Inviting Nonthreatening | Neat Clean Efficient | Bright Alert Exacting coloration |
| Applications | Restaurants Hotel lobbies Boutiques Libraries Office areas Retail stores | Public reception areas Showrooms Bookstores Office areas | Conference rooms Classrooms Hospitals Office areas Mass merchandisers | Galleries Museums Jewelry stores Medical exam areas Printing companies |
| Lamps | Fluorescent Incandescent Halogen | Fluorescent Mercury vapor | Fluorescent Mercury vapor Metal halide | Fluorescent Mercury vapor Metal halide |
| Low- and high-pressure sodium lamps: 1750° K and 2000° K. | | | | |

FIGURE 6-3
Color Temperature

Security personnel need the ability to accurately describe color. It is an important aspect in the apprehension and prosecution of criminals who are caught on CCTV displays and recordings. The ability of a lamp to faithfully reproduce the colors seen in an object is known as color rendition and is measured as a color rendition index (CRI) on a scale of 0 to 100. A CRI of 70 to 80 is considered good, above 80 is considered excellent, and 100 percent is considered daylight. Figure 6-4 shows the CRI values of various lamps. High- and low-pressure sodium and mercury vapor light sources have very low CRI values and should not be used in conjunction with color camera applications or where color identification is critical. Under low-pressure sodium light, a green shirt will have a blue hue.

| Lamp Type | Color Rendition Index |
|----------------------|-----------------------|
| Incandescent | 100 |
| Halogen | 100 |
| Fluorescent | 75-100 |
| Metal halide | 70 |
| Mercury vapor | 50 |
| High-pressure sodium | 20 |
| Low-pressure sodium | 5 |

Figure 6-4
Color Rendition Index

In addition to security operations, high-color rendering is important in retail, restaurant, and precision manual work. A high CRI also increases visual clarity and has been found to create higher morale and greater productivity. High CRI in outdoor locations at night makes pedestrians feel safer because it allows them to see at a greater distance and have better depth perception.

Brightness and glare are more subjective terms. Brightness is the human perception of the amount of light that reaches one’s eyes. Glare is excessive brightness and has importance in security applications. Glare hurts the eye and affects its eye’s efficiency; it creates excessive contrast with other objects, makes people turn their eyes away, and generally makes it difficult to see clearly. Glare can be used effectively to deter unauthorized activity at a site perimeter. However, it has an equally negative effect on patrols and response forces. Additionally, it may cause light trespass onto adjoining properties, including sidewalks and roadways. It is important that light trespass not cause glare or excessive contrast to drivers and pedestrians, both on and off the organization’s property. Many communities set limits, through zoning restrictions, on the level of lighting and the amount of light that can spill onto, or trespass, neighboring areas.

6.2 LIGHTING SYSTEMS

A lighting system consists of a number of components, all of which are important to the effectiveness of a lighting application. Below is a list of the major components and their function.

- The **lamp** (also known as a light bulb) is the manufactured light source that includes the filament or an arc tube, its glass casing, and its electrical connectors. Types of lamps are incandescent, high- or low-pressure sodium, mercury vapor, light emitting diode arrays (LED), and others. The terms describe the type of technology used to create the light.
- The **luminaire** (also known as the **fixture**) is the complete lighting unit, consisting of the lamp, its holder, and the reflectors and diffusers used to distribute and focus the light. Some lamps, such as spots and floods, are designed with integral, shaped reflectors for the focus and distribution of the light. The luminaire also contains the means of connecting to the power source and—depending on the lamp technology—includes ballasts (to generate the correct starting and operating voltage, current, and waveform) and photosensors (to control switching of lights based on ambient lighting conditions). The selection of luminaire depends on aesthetics as well as performance characteristics.
- **Mounting hardware**, such as a wall bracket or light pole, is used to fix the luminaire at the correct height and location.
- **Electrical power** operates the lamp, ballasts, and photocells. Some lamp technologies are sensitive to reduced voltages, in particular the high-intensity discharge (HID) family of lamps (metal halide, mercury vapor, and high-pressure sodium). These lamps require relatively stable voltage levels since they produce light from an arc discharge under high pressure. If the supply voltage is sufficiently reduced, the arc will be extinguished. Restart times are often lengthy (up to 20 minutes). Backup batteries, generators, and uninterruptable power supply (UPS) systems need to be considered for the lighting of high security and safety areas, such as vaults, cash registers, and paths of emergency egress and assembly.

6.3 LIGHTING ECONOMICS

The cost of lighting is a major factor in the level of lighting that will be installed for security and safety. Some lighting is mandated by code. Many times, however, security lighting is an elective cost that must be justified based on identifiable savings or quantifiable reduction in risk.

This section provides some guidance in the cost of operating security lighting. Estimates of the capital costs associated with procurement and installation are best left to a lighting engineer, however. *The Outdoor Lighting Pattern Book* (Leslie & Rodgers, 1996) provides many examples of equipment, maintenance, and energy costs associated with lighting projects for parking structures, office buildings, loading docks, gatehouses, and malls.

For a typical lighting installation, the operating cost consists of capital items (e.g., lamps and ballasts), energy, and maintenance. The proportion of these costs is approximately 8 percent capital items, 4 percent maintenance, and 88 percent energy. The energy efficiency of the lighting is known as a lamp's efficacy and is measured by the lamp's output in lumens divided by the lamp's power draw in watts. The next highest cost is that of replacement lamps and is a function of the lamp technology and the quality of the lamp. Figure 6-5 shows typical levels of efficacy and lamp life. As a ready guide, there are 8,760 hours in a year—a lamp that is on for 8 hours per day will burn for 2,920 hours per year.

The cost figures shown in the last column (McCauley, 1991) represent typical costs to provide 16,000 lumens of lighting for eight hours per day for five years (excluding maintenance and labor costs for cleaning and bulb changes). Electricity is assumed to cost 10 cents per kilowatt-hour (KWH). While lamp prices remain relatively constant, one can easily modify the five-year electricity costs by multiplying the dollar value by the cents per KWH in the area and dividing by 10. For example, the electricity cost for the high-pressure sodium lamp in an area where power costs 15 cents would be $(\$328 \times 15) / 10 = \492 .

Maintenance costs include the labor to replace lamps and to clean them. Cleaning cannot be ignored since the lumen output of a lamp will decline due to dirt accumulating on the fixture over time. In a clean environment, such as a computer room or office area, the percentage of output will decline by approximately 3 to 4 percent per year, and cleaning intervals of three years are recommended. In a very dirty environment, a luminaire could be emitting only 80 percent (a reduction of 20 percent) of its design output after only one year.

Since the power consumption remains the same regardless of the amount of dirt accumulated on the luminaire, it makes sense to implement regular cleaning to maintain the designed light output. It should be noted that the performance of most lamps declines with age. By the end of their rated life they may produce only 80 percent of their designed output, even when clean.

| Lamp Type | Efficacy (lumens per watt) | Life (hours) | Five-Year Cost (lowest = 1, highest = 7) |
|----------------------|--------------------------------------|------------------------|----------------------------------------------------|
| Incandescent | 20 | 1,000-4,000 | 7 |
| Halogen | 25 | 10,000-20,000 | 5 |
| Fluorescent | 60-80 | 10,000-20,000 | 3 |
| Metal halide | 125 | 10,000-25,000 | 4 |
| Mercury vapor | 65 | 16,000-24,000 | 6 |
| High-pressure sodium | 125 | 16,000-24,000 | 2 |
| Low-pressure sodium | 200 | 15,000-25,000 | 1 |

FIGURE 6-5
Lamp Efficacy, Life, and Cost

Lamps need to be replaced as their useful life is reached, and it is less expensive in labor to perform a planned replacement of all, or a group of, lamps rather than wait until they expire individually and replace them one or two at a time. Planned replacement also ensures that there are no dark areas, even for a short time, caused by individual failures. It makes economic sense to use a suitable multiple of the cleaning cycle as the time to re-lamp. For example, if the average useful life of a lamp is six years and cleaning is scheduled every two years, all lamps should be replaced every three cleaning cycles.

The number of luminaires required is a function of the area to be covered, the light levels required, the height of the luminaires and their design, and the type of lighting technology used. Achieving a uniform distribution of light, particularly outdoors, is expensive. Some variation in light levels is considered acceptable and is measured as uniformity, the ratio between the average light level and the minimum light level. Typical uniformity ratios would be 1:0.7 for working environments, 4:1 on a pedestrian walkway, and 10:1 on a roadway. Higher uniformity gives better depth perception and a greater perception of security to individuals in the area.

6.4 **STARTING AND RESTRIKE**

Some lamps require time to relight if they are switched off intentionally or by a full power failure or a brownout. The extended relighting time is typical of high-intensity discharge (HID) lamps since they rely on an arc to produce light. The lamp tube must cool sufficiently before the arc can be restruck. In addition, HID lamps (and to a much lesser extent fluorescent lamps) take time on starting from cold to reach their designed light output levels.

These functional limitations of lamps are of concern to the security practitioner. Although lamp switch-on times can be scheduled to allow for their startup time, a full or partial power failure, however brief, can mean a loss of lighting for a considerable period. Figure 6-6 shows typical starting and restrike times for different types of lamps.

| Lamp Type | Start Time (minutes) | Restrike Time (minutes) |
|------------------------------------------------------------------------------------|-------------------------|----------------------------|
| Incandescent | Instant | Instant |
| Halogen | Instant | Instant |
| Fluorescent | Instant* | Instant |
| Metal halide | 5-8 | 10-20 |
| Mercury vapor | 5-8 | 10-20 |
| High-pressure sodium | 2-5 | 1-20 |
| Low-pressure sodium | 5-8 | 0-8 |
| * Fluorescent lamps require time to reach full output, especially in cold weather. | | |

Figure 6-6
Lamp Starting and Restrike Times

New technology and manufacturing methods seek to reduce these times. For example, some HID lamps are available with two tubes. Only one is used at a time, so the other remains cool for a quick restrike.

6.5 SECURITY LIGHTING APPLICATIONS

The security professional needs to consider lighting in a number of different areas of the facility being secured. A general rule for lighting levels is 0.5 fc for detection, 1.0 fc for recognition, and 2.0 fc for identification (McGhee, 1988). The following list provides a sample of types of areas together with lighting recommendations:

- **Perimeter fencing.** Lighting, as well as physical barriers, can act as a deterrent to unauthorized intrusion. If perimeter intrusion detection systems are used, the lighting also aids in the use of CCTV systems for alarm assessment and helps the response force delay or apprehend the perpetrators. NRC regulations specify 0.2 fc of illumination at the perimeter and in the clear area between the two fences. Since the perimeter fence may border on the property of neighbors, light trespass needs to be considered in the design solution.
- **Site landscape and perimeter approaches.** Roadways and pedestrian walkways are lit for both safety and security reasons. Vertical lighting, shining onto the horizontal walkway or roadway, is ideal for identifying potholes or objects that may cause tripping. However, when installing lights so pedestrians can see each other, or for the most effective use of CCTV cameras, some component of the light must be horizontal to illuminate vertical surfaces. Site landscapes are particularly difficult and expensive to light, especially if trees and shrubs provide cover to would-be intruders. Ground lighting focused up into the trees and shrubs is most effective in deterring their use as hiding places. Such lighting also provides a high-contrast background to detect movement. Typical lighting levels are 1-4 fc for walkways, 0.5-2 fc for roadways, 10 fc for entrances and 2 fc for open yards.
- **Building facade.** Where individual exterior objects cannot be adequately lit, providing a high contrast will give good identification of shape and movement. The floodlighting of a building facade achieves this goal. If the facade has good reflectance, there will also be a measure of horizontal light for a viewer (person or camera) located between the facade and the object to identify the object. Typical lighting levels for security are 0.5-2 fc.
- **Parking structures.** These areas are difficult to light since there are few vertical elements to reflect light or provide contrast to moving objects. In some municipalities, building codes require a bright white horizontal stripe on walls, at waist height, to improve contrast. The lack of ceiling clearance restricts the height of luminaires and requires the fixtures to spread the light horizontally. This is excellent for lighting vertical surfaces; however, if CCTV cameras are used, the luminaire design should be selected to reduce glare at the camera lens. A horizontal illuminance level of 5 fc with a uniformity ratio of 4:1 provides an adequate level of security.

- **Open parking.** The height of luminaires is less restricted in open than in covered parking unless local codes and light trespass become factors. The higher light sources tend to provide horizontal illumination. Recommended light levels range from a minimum of 0.2 fc in low-activity general parking and pedestrian areas to 2 fc in high-activity vehicle areas. Cash collection and vehicular access control areas should be maintained at a minimum of 5 fc.
- **Loading docks.** Nighttime lighting depends on off-hours activity. To maintain an adequate level of security for the exterior area without truck parking, 1 fc at the building facade (roll-up doors, stairs, ramps, etc.) and 0.2 fc in open yards is recommended. For nighttime shipping and receiving operations, the illuminance should be increased to 5 fc. Interior dock areas, such as loading bays, should be lit to 15 fc, and unpacking and sorting areas to 20 fc. Packing and dispatch areas are recommended at 30 fc.
- **Security control and monitoring rooms.** Most activities in this area are computer-based and should be illuminated to 30-50 fc with task areas, such as a console desk, at 50 to 70 fc. Glare from computer and video monitoring screens can be a problem. The positioning of luminaires and the angle of screens are critical in minimizing glare. The type of screens used is also important: Flat screens and ones with anti-glare coatings or covers will help to reduce or eliminate glare. If screen monitoring, e.g., alarm and CCTV, is the predominant function, monitoring staff may want to reduce the ambient light levels considerably to minimize glare and increased the contrast of the screens. The security manager should discuss the use of dimmers with the lighting designer.
- **Guard and gate houses.** The area surrounding a gate or guard house should be well lit, 2-5 fc, on the exterior at night. Task lighting on the interior should be high, 30 fc, during daytime operations, but should be reduced at night to below exterior levels to permit good visibility of the surroundings and approaching pedestrian and vehicular traffic. Figure 6-7, based on Leslie and Rodgers (1996) summarizes the perceived level of security at different lighting levels for various applications. The authors provide practical examples of how lighting can be improved and notes capital and operating costs for each type of upgrade. With a proper lighting design, increased lighting increases security.

| Application | Average Horizontal Illuminance (footcandles) | Sense of Security (1=poor, 5=best) |
|----------------------------|-----------------------------------------------------|-------------------------------------------|
| Pedestrian Mall | | |
| Typical | 0.43 | 2 |
| Upgrade | 2.00 | 4 |
| Redesign | 3.80 | 5 |
| Office Park | | |
| Typical | 0.96 | 2 |
| Upgrade | 1.70 | 3 |
| Parking Structure | | |
| Typical | 0.93 | 2 |
| Upgrade | 1.90 | 3 |
| Redesign 1 | 3.00 | 3 |
| Redesign 2 | 4.10 | 4 |
| Redesign 3 | 5.20 | 5 |
| Loading Dock (Exterior) | | |
| Typical | 0.99 | 2 |
| Upgrade | 0.65 | 3 |
| Redesign | 1.30 | 4 |
| Guardhouse | | |
| Typical | 1.00 | 1 |
| Upgrade | 1.40 | 3 |
| Redesign | 4.30 | 5 |
| Gatehouse | | |
| Typical | 0.46 | 1 |
| Upgrade | 1.00 | 3 |
| Redesign | 2.30 | 5 |
| Campus Green | | |
| Typical | 0.33 | 2 |
| Upgrade | 0.61 | 3 |
| Redesign | 1.50 | 4 |
| Urban School (Three-Story) | | |
| Typical | 0.41 | 1 |
| Upgrade | 0.68 | 2 |
| Redesign 1 | 2.70 | 4 |
| Redesign 2 | 2.30 | 4 |
| Rural School (One-Story) | | |
| Typical | 0.77 | 1 |
| Upgrade | 0.99 | 3 |
| Redesign | 1.20 | 4 |

Figure 6-7
Lighting and Security Perceptions

6.6 **SECURITY LIGHTING AND CLOSED-CIRCUIT VIDEO SYSTEMS**

Where CCTV cameras are used to augment security, some additional lighting considerations apply:

- color rendering index (CRI) for accurate reproduction and identification of colors
- reflectance of materials
- directionality of the reflected lighting

Another important factor is the wavelength of the source illumination. The human eye, by definition, sees light in the visible spectrum, which has a bandwidth between 400 nanometers (nm) (violet) and 700 nm (red). The electromagnetic spectrum, of which the visible spectrum is only a small part, has a much larger range, but human eyes are not sensitive to it. Close to either end of the visible spectrum are the ultraviolet and infrared wavelengths. Both the sun and artificial lighting sources produce energy beyond human sensitivity. CCTV cameras are generally designed to see what people see, but many cameras can sense illumination in the near-infrared range (700 nm - 1,100 nm). The use of an infrared (IR) light source in conjunction with a camera incorporating a special sensing element, such as Ex-wave CCD, allows views to be displayed even where there is no visible light. This is useful where zoning restrictions limit the amount of light trespass or where covert surveillance is desired. The use of IR illuminators is limited to monochrome, not color, cameras. The IR luminaire should be co-located with the camera and should be chosen to provide a beam spread consistent with the camera lens setting. For dynamic (pan/ tilt/zoom) cameras the IR source can be mounted on the pan/tilt mechanism to follow the direction the camera is pointing. The design should ensure that the pan/tilt is rated for the weight of the camera plus the luminaire.

The color temperatures of various light sources were shown in Figure 6-3. Most cameras' data sheets state their performance based on an incandescent tungsten filament (2,700° K) light source. None of the color cameras generally used for CCTV are effective at the 1,700° K range of low-pressure sodium lamps, but newer CCD elements, such as the Hyper HAD, considerably improve the color rendition of a scene illuminated by high-pressure sodium light (2,200° K).

In general, color cameras require twice the light that monochrome cameras need for the same picture quality. In addition, a color camera needs at least 50 percent of its full video signal or color registration starts to fade, whereas black-and-white need only 20-30 percent of full video.

Several other specifications from camera data sheets are as follows:

- Minimum light levels are quoted at 75 percent or 89.9 percent reflectance.
- Minimum light levels are quoted for specific lens characteristics. For example, a standard color camera may perform at a minimum illumination of .25 fc with an f/1.2 lens; with an f/2.0 lens, the minimum illumination increases to .68 fc, an increase of 2.7 times the lighting level. The selection of lens and its quality is important.
- White balance is the automatic adjustment within a camera for the color temperature of the light source. This parameter can range from 2,200° K to 7,000° K. The range of white balance of the camera should be compatible with the existing or designed lighting.

6.7 STANDARDS FOR SECURITY LIGHTING LEVELS

The first national standard was issued in 1942 and was modified and sponsored by the Illuminating Engineering Society of North America (IES) as ANSI A85.1, American National Standard Practice for Protective Lighting, in 1956. It was reaffirmed in 1970 but has since been withdrawn.

IES's *Lighting Handbook* (1993) contains Chapter 33 "Emergency, Safety and Security Lighting." IES also publishes numerous lighting design guides and recommended practices for applications like roadways (RP-8-1983), parking facilities (RP-20-1985), automatic teller machines (DG-9-97), bikeways (DG-5-94), and exterior environments (RP-33-99). Other sources of lighting standards are the *U.S. Army Field Manual* and regulations from the Nuclear Regulatory Commission (NRC) governing licensees who possess special nuclear materials. These bodies describe significantly different standards for minimum lighting levels, which can cause confusion for security managers, systems designers, and architects. Minimum lighting levels are offered in Figure 6-8. They are extracted from a number of sources and are intended for use only as a guide.

| Application | Minimum Lighting Level— IES Standards (footcandles) | Comments/Other |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------------|
| Perimeter fence | 0.50 | NRC 0.20 fc |
| Outer perimeter | 0.50-2.00 | NRC 0.20 fc; DoAFM 0.15 fc |
| Open area | 2.00 | |
| Open parking lot | 0.20-0.90 | IES high vehicle activity 2.00 fc |
| Covered parking structure | 5.00 | |
| Pedestrian walkway | 0.20 | IES 7.50 fc at ATMs |
| Pedestrian entrance | 5.00 | DoAFM 2.00 fc |
| Vehicle entrance | 10.00 | DoAFM 1.00 fc |
| Building facade | 0.50-2.00 | |
| Gatehouse | 30.00 | |
| Loading dock exterior | 0.20-5.00 | |
| Loading bay | 15.00 | |
| Office—general | 30.00-50.00 | |
| Office—task | 50.00-70.00 | |
| Interior public area | 10.00-20.00 | |
| Retail store | 50.00 | |
| Bank—lobby | 20.00 | |
| Bank—teller | 50.00 | |
| Bank—ATM | 15.00 | IES 30 fc on preparation counter |
| IES=Illuminating Engineers Society of North America NRC=Nuclear Regulatory Commission DoAFM=Department of the Army Field Manual fc=footcandles | | |

Figure 6-8
 Guidelines for Minimum Lighting Levels

REFERENCES

- Greenwoll D. A. (1991). *An evaluation of intensified solid-state video cameras*. SAND90-2566. Albuquerque, NM: Sandia National Laboratories.
- Lighting handbook*. (1993). New York, NY: Illuminating Engineering Society of North America.
- Leslie, R. P., & Rodgers, P. (1996). *The outdoor lighting pattern book*. New York NY: McGraw-Hill.
- McCauley, M. L. (1991, September). Lighting principles. *Security*.
- McGhee, T. (1988, March). Spotlight on the night. *Security Management*.
- McGhee, T., & Pierce, C. (1990, December). Lighting the way to security. *Security Management*.
- Phillips Lighting Company. (1999). *Lamp specification and application guide*.
- U.S. Army field manual*. (1979). Washington, DC: U.S. Government Printing Office.

Note: SAND documents may be obtained at <http://www.osti.gov/bridge/advancedsearch.jsp>.

CHAPTER 7

ALARM COMMUNICATION AND DISPLAY

Alarm communication and display (AC&D) is the part of a PPS that transports alarm and assessment information to a central point and presents the information to a human operator. New developments in electronic and computer technology have changed the design of alarm communication and display systems over time. It is now possible to quickly collect and process a wide variety of information; the challenge is to effectively present this information to a human to help him or her make a decision about what actions are needed. This chapter describes equipment and techniques available for reporting alarms to an operator, focusing on the intrusion detection functions of an AC&D system.

The two critical elements of an AC&D system are

- the transportation or communication of data, and
- the presentation or display of that data to a human operator in a meaningful manner.

7.1 AC&D ATTRIBUTES

The most useful AC&D systems have certain characteristics. Systems must be designed to withstand the environments in which they are placed. If a component will experience wide temperature variations, such as in an exterior environment, the equipment must be designed to withstand those variations without failing. Robustness is a measure of system performance in all probable environments.

AC&D components and systems should be designed to last a long time. The individual components should be reliable and have a long mean time between failure (MTBF). A reliable system requires less maintenance and is more trusted by operators. Other aspects of reliability include reliable communication and display of alarm data and no loss of information. No communications system has 100 percent guaranteed information delivery; however, modern communications equipment can approach that goal by implementing techniques for checking and verifying data.

Electronic components eventually fail. Good AC&D systems take the chance of failure into account and provide redundant or backup capability for critical components. By maximizing the robustness, reliability, and redundancy of AC&D systems, the time an AC&D is inoperable or down for repair can be minimized.

Alarm information must be available to security personnel in a timely manner. The AC&D system speed should be a small fraction of the overall alarm assessment and response force time. These times will vary from site to site, but AC&D speed should be a negligible factor in calculating response or assessment times.

The AC&D system is a major component in the overall PPS. Because the PPS protects the site's critical assets, it follows that the AC&D system must be secure from attacks by adversaries. For example, procedures should limit who has access to AC&D displays and the system configuration, and only authorized persons should have access to AC&D information, components, and wiring. As part of this protection, the alarm communication subsystem should also be secured from access by attackers.

AC&D systems must be easy for an operator to use. While a multitude of sensors can provide considerable data, this data must be displayed in a fashion that presents the essential information to the operator. In addition, the user must not be overwhelmed with data, interaction with the system must be efficient, and users must be able to perform necessary operations quickly and easily. A system that is easy to use also reduces the amount of training and retraining needed.

Each of these general characteristics plays a part in the overall effectiveness of an AC&D system, but the most important measure of AC&D effectiveness is how well it quickly and clearly communicates alarm data from sensors to the system operator. When an alarm event occurs, the AC&D system must communicate to the operator the following information:

- where an alarm has occurred
- what or who caused the alarm
- when the alarm happened

The operator should also know how to respond. This can be accomplished through training and AC&D system prompts. Moreover, all AC&D activity must occur in a timely fashion, so AC&D system speed is a measure of its effectiveness.

The difficulty with this effectiveness measure is its relationship to the response time of a human operator. Measuring operator response is a very difficult process. Electronic communications systems, on the other hand, are quantifiable. This dual character of AC&D systems makes measuring system effectiveness more complex. Communications systems can be understood, network topologies modeled, and system times measured. With humans, however, softer sciences such as ergonomics, human factors engineering, and physiology studies are also needed.

The AC&D system is divided into several subsystems: communications, line supervision and security, information handling, control and display, assessment, and off-line subsystems. These are discussed in detail below.

7.2 **ALARM COMMUNICATION SUBSYSTEM**

The communications subsystem transfers data from one physical location to another. Specifically, an AC&D communications subsystem moves data from the collection point (sensors) to a central repository (display). If the central repository consists of multiple computers or displays, then the communication subsystem may also move data throughout the repository.

The basic concepts of AC&D communications incorporate a design model, detailed system functions and how they relate to the other AC&D requirements, size of the system and the topologies used, and the combination (in hierarchies) of simple system configurations. Alarm communication systems have several characteristics that drive the design. These characteristics include the quantity of alarm data, high reliability needed for the system, and speed at which data must be delivered. The following discussion details each of these system characteristics and describes the role of these characteristics in system design.

If a sensor activates, the alarm communications system must make sure accurate data pertaining to the activation is received by the AC&D computers. Assured message delivery means the communication system must be reliable. In addition, alarm data must be transmitted in a timely manner. Both human-factor considerations and interactions between the AC&D and assessment systems drive alarm reporting speeds.

Human factors require alarms to be reported with no perceptible delay. For an operator, no perceptible delay is a few tenths of a second. Interactions between the AC&D and the assessment system require reporting times to be a small fraction of the total assessment time. While total assessment times can vary widely, AC&D and assessment system interaction should only take milliseconds. Such reporting speeds require fast alarm communications since communications times are only a part of the total alarm reporting time.

Other factors are also important when designing an effective alarm communication system. Physical media must have sufficient bandwidth to handle the communications for the system when operating at full capacity. Protocols, or the special set of rules for communicating that the end points in a telecommunication connection use when they send signals back and forth, are important components of system design. System speed dictates the types of protocols used in the system, and protocol overhead must be appropriate for the types of data being transmitted. In addition, channel bandwidth and protocol overhead must be balanced to provide the required system speed.

The best possible communications system would provide instant communications with 100 percent reliability. In reality, it is not possible to meet that standard. Moreover, high-speed, high-reliability systems are expensive. A good communication subsystem design balances the cost of the system with its performance. Depending on the design, a range of protocols can be used to balance speed, reliability, and cost.

To ensure that messages reach the operators in the highest-security or most complex systems, redundant hardware is required to handle cases of hardware failure, and the system must be able to automatically route messages through the redundant hardware as required. In addition, the protocols used should detect and correct message errors and duplicate messages.

7.3 **SECURITY COMMUNICATIONS**

Numerous vendors offer a broad range of telecommunications services using a wide variety of technologies. A major task for the assets protection professional is addressing relevant concerns when considering a communications application. The task will be complicated by the expanding range of available communications technology.

For many applications, the communications media of choice are optical fiber or satellite rather than copper wire. Optical fiber is less expensive than copper wire and provides security, high-speed transmission, and versatility. It is the cable of choice for terrestrial

communications carriers. Satellite technology—versatile and particularly useful in developing areas—has experienced explosive growth.

In every communication, security professionals are concerned with the following

- integrity of the communications medium (availability of the message path)
- integrity of the message (complete and errorless transmission of the data)
- timeliness of the transmission (data communication within an appropriate time frame)
- message security (accessibility of the communication to authorized persons only)

The sections that follow address verbal and nonverbal security communications, including status and alarm monitoring, access control, and video surveillance. They also examine wire, radio, microwave, and light as communication media in terrestrial and earth satellite configurations.

7.3.1 **WIRE AND CABLE COMMUNICATIONS**

Alarm signals may be transmitted on an unshielded pair of direct current (DC) conductors. The size of the wire and its resistance must be considered because resistance varies directly with the length of the line and inversely with the diameter of the wire. The effective length of a line is limited by the wire resistance.

Audio transmissions require the use of shielded twisted pairs of alternating current (AC) wires, referred to in telephone parlance as voice-grade lines. Alarm signals and audio transmissions may both be transmitted on the same pair of twisted, shielded wires.

Signals also may be transmitted on lines installed to carry electric power. In the United States, power is usually transmitted at 60 Hz (cycles per second). In other countries, the transmission may be at different frequencies. A device can be installed on the line to couple the higher-frequency communication signals to the AC wire path. At the receiver, the frequencies above 60 Hz are separated and displayed or recorded, while the normal 60 Hz electrical current is undisturbed. The communication path may be blocked at an AC power transformer, and interference on the AC wire path may degrade or garble the signal frequencies.

Optical Fiber

The capability of optical fiber to transmit extremely large volumes of information at the speed of light has revolutionized the communications industry. This signal-carrying capacity makes it possible to transport more sophisticated signals than could ever be handled by a like amount of copper wire. (A system operating at 565 Mbits—565,000,000 bits per second—

can support 8,064 telephone conversations per fiber.) Transmission technologies can support virtually any combination of video, data, and audio transmitted one at a time or simultaneously, one way or two ways over a single fiber.

An optical fiber is a strand of high-purity spun glass, typically about the thickness of a human hair. A light source, such as a laser or a light-emitting diode (LED), introduces a modulated light beam into the fiber and is carried, essentially unattenuated and unchanged, to a unit at the other end, in which the modulated beam is decoded and the original information recovered. The LED is the light source of choice. It has a longer lifetime without maintenance and is less sensitive to fluctuations in the power source and to changes in temperature and humidity.

Optical fibers can be used to carry voice-grade signals, video signals, and digital or data grade signals. Optical fibers differ from conventional metal wire in several ways:

- They are not affected by electromagnetic interference (EMI) or radio frequency interference (RFI).
- They do not carry any electrical current and do not radiate signals.
- They can carry many more different multiplexed messages than conventional wires.
- They are much smaller and lighter than conventional wires.
- They are flexible and can take an irregular course from point to point.
- They are not vulnerable to interception by acoustical or inductive coupling.

Video Transmission

Video signals cannot be transmitted directly on DC lines. However, video can be transmitted on coaxial and optical fiber cable, on standard telephone lines, or on balanced twisted-wire pairs.

For coaxial cable transmission, the video signal does not require further processing between the camera and the monitor if the transmission distance is short enough, typically 1,000 ft. (305 m). Longer transmissions can be achieved if the signal is amplified along the way.

Video signals that are transmitted via normal telephone circuits are first converted to digital, then to audio signals. The audio is reconverted to video at the receiving end. Telecommunications providers continuously amplify transmission circuits; thus, there is no theoretical limit to the distance of such transmissions. The signal can be moved from wire to microwave to satellite paths, as required by the telephone switching control.

For optical fiber transmissions, conversion from video to optical signals is required at the transmitter, with reversion at the receiver. The transmission distance without amplification is 1 mile (1.6 km) or more. If the transmission path is via optical fiber and the telephone signal is in digital format, real-time transmission is possible because the optical fiber can transmit more data faster than standard telephone copper wire pairs.

The systems will support color or monochrome video equipment. Data signals to control the pan/tilt driver, zoom lens, and auxiliary equipment, such as housing heaters and wipers, are transmitted to the camera location over the same optical fiber that is transmitting the video signal. Three functions can be transmitted simultaneously in two directions on one fiber.

Video may be transmitted on dedicated twisted-wire pairs, provided there is no bridging or coupling and there are no other connections on the wire path between the video transmitter and receiver. Video also can be transmitted if the equipment used can perform required conversions and impedance matching and frequency compensation to assure a usable video signal. Good performance can be achieved at wire distances of up to 4,000 ft. (1.2 km).

Status and Alarm Transmission

Three types of line transmission installations usually are used in electronic protection systems: loop, point-to-point, and multiplex. The three types may be used with proprietary wire networks or leased telephone lines. With any alarm system configuration, access to the control unit would permit disabling the entire system; thus, physical security of the control unit or console is critical.

Loop

In a loop system, devices are installed on a pair of wires that have been looped throughout an area, a building, or a facility, and then connected to a control center. A signal at the control center indicates when an abnormal situation occurs on the loop. This system may be adequate for a small space or a single facility; however, the better method is to code the signal from each detector so that the source of each signal can be defined at the central point.

A short circuit or broken connection on the loop may interrupt all signals on the far side of the break. This problem can be partially corrected by using a McCulloh circuit. In this circuit, when an open occurs, the circuit is switched to send current from the control unit over both sides of the circuit wires out to the break point. The circuit integrity is thus restored to all devices on either side of the open. If two circuit breaks occur, any devices between the two breaks will be lost, as there will not be any circuit path between the breaks.

Point-to-Point

Each sensor in a point-to-point installation is connected directly to a control center by a pair of wires. This hard-wired installation is more expensive than the loop system because more wire is required; however, only one detector is influenced in case of an individual line fault. An attacker attempting to disable the system would have to define each wire controlling each sensor in the area to be penetrated, and each alarm line would have to be disabled. With the loop system, all the detectors in an area could be disabled by interrupting the loop at the proper location.

Multiplexing

Multiplexing is a technique to transmit several messages simultaneously on the same medium. A large number of signals can be encoded into one composite signal for transmission on a single circuit (Figure 7-1.) At the receiving end, the signals are separated and routed to a control unit so they can be recorded and displayed. The transmission medium can be wire, radio frequency (RF), microwave, or optical fiber. A multiplex installation can be more cost-effective than a loop or point-to-point installation, as multiple signals are transmitted over longer distances to a control center. As the number of remote data sources or sensors increases, a loop system or a separate transmission line for each becomes less practical. However, multiplexing equipment is expensive, and it cannot be assumed that multiplexing is less costly. A cost analysis should be made for each system.

Interruption or destruction of a multiplexed communication link results in the interruption of all signals on that link. With large installations or high protected values, a redundant communication path is desirable so that if the main multiplex path is disrupted, the signals will not be lost. The redundant path can be an alternate multiplex trunk, a digital communicator using telephone circuits between remote transponders and the console, or an RF link between the transponders and the console. The cost of the redundant transmission path must be included in the cost-benefit analysis of any system. Considering the great reduction in wiring labor costs, multiplex installation usually has an advantage over hard wire. (Figure 7-2 indicates the process sequence for a multiplex transmission.)

Individual signals in the multiplexing process share a common transmission path but must be separated so they do not interfere with each other. The two methods generally used are (1) time separation or time division multiplexing (TDM), and (2) frequency separation or frequency division multiplexing (FDM).

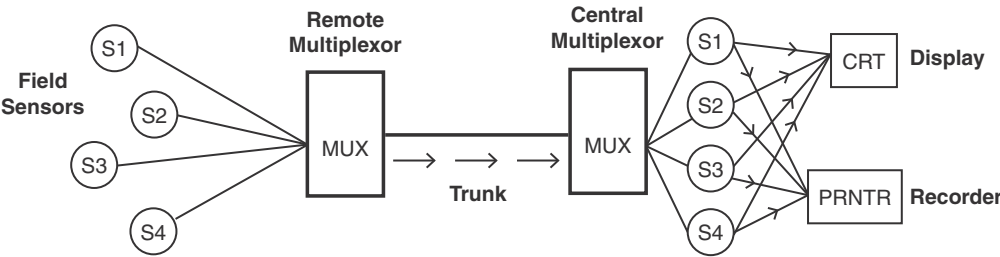


Figure 7-1
Multiplexing on a Pair of Wires

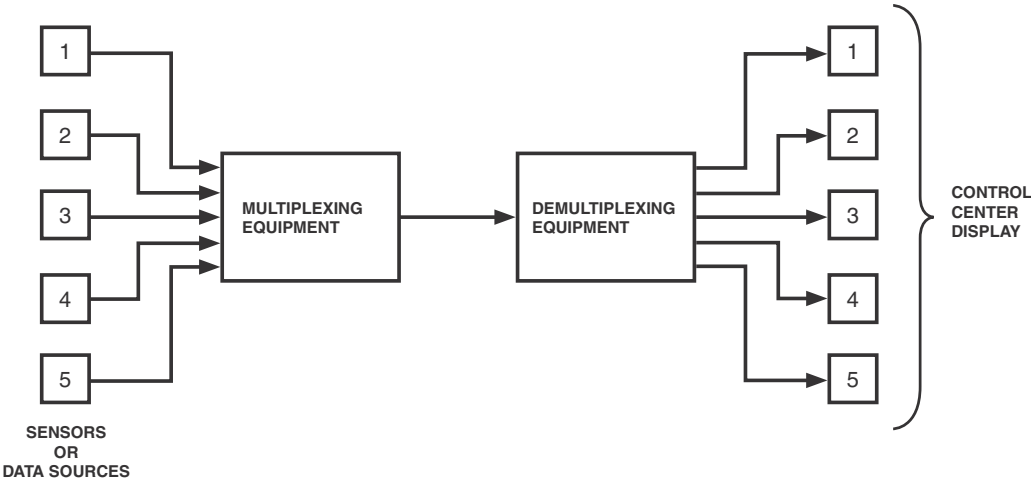


Figure 7-2
Elements of Multiplexing

With TDM, each sensor or data source is assigned a time segment and each may transmit only during its assigned segment. The different signals use the same transmission path, but not simultaneously. The signal in each channel is sampled in regular sequence. When all the channels have been sampled, the sequence starts over with the first channel. Since no

channel is monitored continuously in a time division system, the sampling must be rapid enough so that the signal amplitude in a particular channel does not change too much between samplings. The electronic transmission speeds make the actual small time variances transparent to control or monitoring personnel (Figure 7-3.)

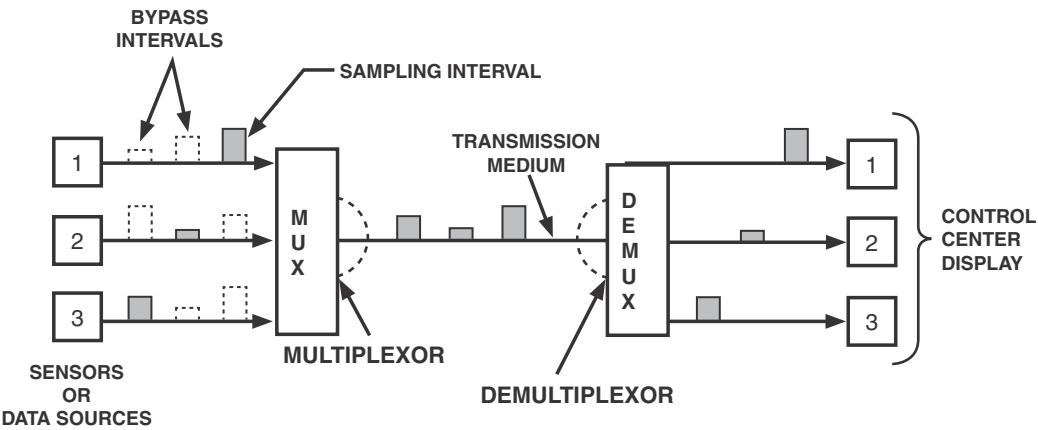


Figure 7-3
Simplified Time Division Multiplex System

In FDM, signals from a number of sensors on a common transmission line occupy different portions of the frequency spectrum. Even though transmitted simultaneously, their different frequencies keep them individually identifiable at the receiver. An example of frequency division multiplexing would be a system where three transducer outputs modulate three subcarrier frequencies (Figure 7-4).

The oscillator for channel 1 is centered at 400 Hz, and the applied data signal produces a peak deviation of ± 30 Hz. Channel 2 is centered at 560 Hz, its peak deviation is ± 42 Hz, and channel 3 deviates ± 55 Hz around a center frequency of 730 Hz. These three channels can be placed on a common transmission medium to form a frequency band ranging from 370 Hz to 785 Hz. There is no overlapping between channels, and unused guard bands between them ensure separation.

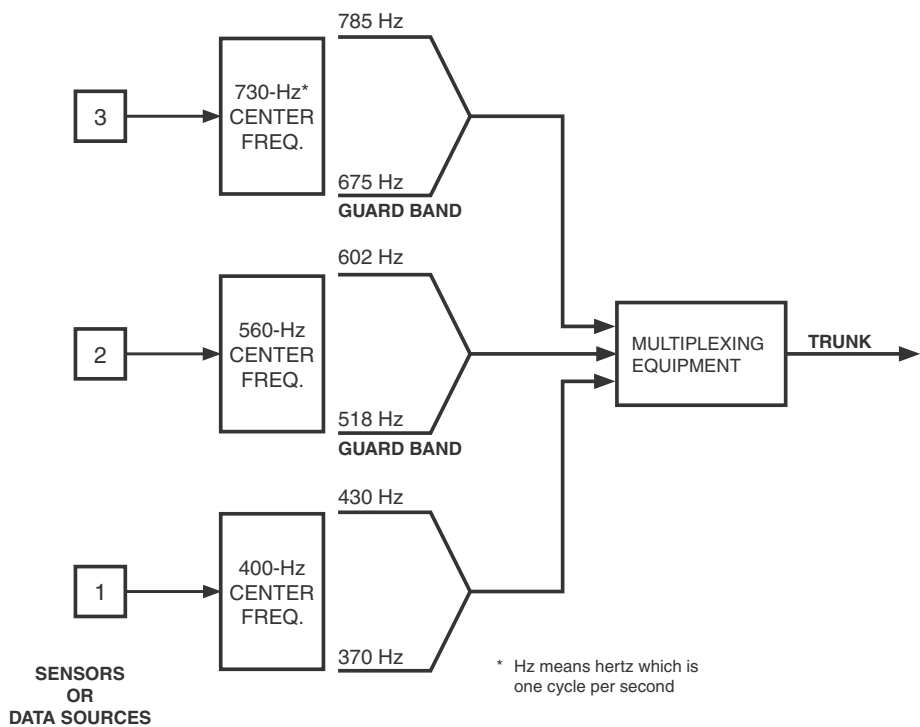


Figure 7-4
Typical Arrangement for Frequency Division Multiplexing
(Channels Separated by Unused Guard Bands)

At the receiving end of the system, bandpass filters separate the channels, sending them to individual discriminators for demodulation and recovery of the original signal. The output of each discriminator terminates at a control center display.

With either type of multiplexing, the receiving demultiplexor must be operating at exactly the same frequency as the multiplexor to distribute the parts of the multiplexed signal to the proper output device at the control center. Because a time division system is based on precise timing, it is vitally important that both multiplexors and demultiplexors are synchronized exactly.

7.3.2 **WIRELESS COMMUNICATIONS**

A wireless communication requires the following:

- a transmitter to furnish radio frequency energy
- an antenna to radiate the energy into the atmosphere
- a receiver
- power for the transmitter and receiver

The transmitter modulates or varies a carrier wave to create different values, which represent the signal characteristics of the source. Modulation is either amplitude modulation (AM), in which the variations are in the amplitude or range of the carrier signal, or frequency modulation (FM), in which the variations are in the carrier frequencies. The receiver resonates or tunes the signals, amplifies them, and demodulates or detects the original source signals to be reproduced by a printer or loudspeaker.

Any unscrambled or unencrypted communication transmitted by wireless technology should be considered available for interception.

Voice Radio

Voice radio is used in many protection systems. A base transmitter station usually is located at the control center, where all other alarm system signals terminate. Security personnel who require communication with the control center use mobile or portable units. All units that will communicate directly with each other must be on the same frequency. However, a base unit using several frequencies can relay data to and from units that do not share a common frequency.

The required output power level and commensurate cost of the equipment is determined by the desired transmission distances, physical barriers that are present, and signal interference in the area. In addition to more powerful base station and receiver equipment, repeater stations or remote transmitters might be required. These receive and amplify the original signal and retransmit it.

Wireless Alarm Signals

A wireless alarm system at a protected site consists of an alarm detection array and an RF interface module. The system vendor provides a network of RF receiver sites, or base stations, which are linked by redundant leased lines to the vendor central station. Some vendor networks consist of thousands of base stations, which provide the service essentially nationwide. When an alarm sensor is activated, a coded alarm signal is transmitted by an omnidirectional antenna to all base stations within range of the transmitter. The base station

receiving the strongest signal transmits the alarm via a leased line to the central station. The central station sends an acknowledgment of receipt of the alarm to the control panel at the protected site using the same channel on which the alarm was transmitted.

The system provides for selection of RF or digital wire. In dual mode, the alarm signal is transmitted simultaneously over both communication paths. The central station can poll the system at regular intervals to ensure functionality.

Cordless Telephones

Cordless telephones usually are not used in security operations, but a security-related call to an executive residence could be answered using a cordless set. The set consists of base and handset transceivers, between which the communication is transmitted by radio frequency. The transmission range is nominally 700-1,000 ft. (213-305 m); however, with some sets or certain atmospheric conditions, the signals can be received over greater distances. While U.S. laws prohibit the interception of cordless telephone transmissions, listening to the cordless telephone calls of a neighbor is not uncommon. Cordless telephones operating in certain frequency ranges offer more security. Some sets also offer security codes and multiple frequency settings. A basic rule is that sensitive information should not be discussed on any cordless telephone call.

Cellular Telephones

Cellular telephone technology has revolutionized telecommunications throughout the world. In some countries, where the wired telephone network has not been developed, several generations of technology have been bypassed and digital cellular telephones are in widespread use. The basic operating principle is to provide the mobile user with a radio link, via a computer-controlled switching center, with the landline network or another mobile unit.

In the cellular concept, service areas are divided into cells, which are grouped in clusters. The cells can be any shape and do not have to be uniform. A group of frequencies is assigned to each cluster, with different frequencies used in adjoining cells. A frequency is not used twice in the same cluster, but the same pattern of frequencies can be used in an adjoining cluster. The power level for each transmitted frequency prevents the signals from reaching cells in other clusters that use the same frequency. At least one cell site serves each cell. A cell site includes low-power transmitters, receivers, a control system, and antennas. Dedicated voice and data trunks link the cells to a computer, which controls cell operations, connects cellular calls to the land line network, captures billing information, and controls unit activity. When a user moves from one cell to another, a call in progress is handed off to the second cell on a new frequency. Thus, a large number of callers can simultaneously use the frequencies in the service area.

Cellular service is available in different formats, which are transmitted in several frequency ranges. In the United States, depending on the technology used, cellular systems use the 800 MHz or 1,900 MHz frequency range. In other countries, the 900 MHz range or the 1,800 MHz range is used. The assets protection professional should not assume that the cellular service in use in one area will be compatible with the service offered in another area. Multiple-frequency cellular telephones can resolve many compatibility problems.

Signal Compression

Telecommunications providers use two forms of digital transmission compression to maximize the use of spectrum space in both cellular telephones and personal communications systems—called time division multiple access (TDMA) and code division multiple access (CDMA). These technologies are not compatible with each other.

TDMA divides calls into pieces of data that are identified on the receiving end by the time slots to which they are assigned. TDMA enables one cellular channel to handle several calls simultaneously.

CDMA spreads segments of calls across a wide swath of communications frequencies. The segments carry a code, which identifies the originating telephone. The receiving equipment uses the attached code to identify and reconstitute the original signal. Digital CDMA offers 10 to 20 times the capacity of analog cellular transmission.

Cellular service can be used in many ways:

- as a backup to the wire network for alarm transmissions
- in a disaster where the wire network is disrupted
- in a hostage situation
- as a backup to routine security communications

Scrambling

The security of a communication can be enhanced by the use of scramblers. This technique is applicable to a cellular conversation. Normally, a scrambler is required at both the originating and terminating locations. However, a telephone privacy service vendor can provide a specialized service in which the customer requires only one scrambler. Using a telephone to which a telephone privacy device is attached, the customer calls a toll-free number at the vendor site, where a similar device is installed. From that point, the privacy network provides another dial tone and the user dials the desired terminating number. The conversation is scrambled by the privacy device on the originating telephone and unscrambled by the privacy network device. The voices of both parties to the communication are secure through the cellular network to the privacy service switch equipment.

Two cellular sets equipped with privacy devices also may call directly to each other for secure communication. Only calls requiring privacy need to be made through the privacy service or scrambled between two device-equipped cell phones. Other calls can be made normally through the cellular service provider equipment. Secure calls may be made and received both domestically and internationally. The privacy service vendor also can assign a private toll-free number to a subscriber to enable the receipt of secure incoming calls. A landline version of the privacy device is available for office or home telephones, and the devices are compatible with fax machines.

Analog Cellular

Analog cellular, or advanced mobile phone service (AMPS), transmissions in the United States are in the 800 MHz frequency range. In many other countries, AMPS is not compatible with the local cellular technology. The analog transmission is normally sent “in the clear” and can be used immediately by a person intercepting the signal.

Digital Cellular

Digital cellular service (DCS) transmissions in the United States are in the 1,900 MHz frequency range. This service is also known as personal communication service (PCS). In most other countries, digital cellular transmissions are either in the 900 MHz or the 1,800 MHz range.

In a digital transmission, the analog voice message is converted to a string of binary digits, and interception of the signal yields a string of bits that cannot be used immediately by the person intercepting the signal. However, the transmission could be recorded and converted to analog format to reveal the message content.

Private Fixed Wireless Systems

A wireless private automatic board exchange (PABX) uses a low-power transmitter to communicate with handheld telephones within a limited range. The major advantage is that two-way communication can be established with an employee whose duties require roaming throughout the facility. As in digital cellular systems, the signal can be intercepted using a receiver tuned to the transmission frequency. The use of transmission compression technology, such as TDMA, adds a measure of security to the system.

Local Digital Fixed Wireless Systems

The U.S. Federal Communications Commission (FCC) ruled that telecommunications providers may compete to provide local telecommunications service. A competing provider would be expected to lease facilities from the local service provider whose cables are already in place.

One major telecommunications provider has developed a digital fixed wireless system in which low-power transmitters serve a number of properties in a limited area. The transmitter communicates with a device installed in each property to send and receive voice and data. The system eliminates the need to install or lease wire facilities. The security of the transmitted communications remains to be evaluated.

Satellite Communications

Satellite communications using newly developed technology are growing. Geo-stationary earth orbit (GEO) satellites in current use at high altitudes have an inherent signal delay, which can be a problem in certain communications applications. Delay-sensitive communications will benefit from emerging technology that is used in low earth orbit (LEO) satellite systems.

Satellites transmitting signals to earth cover a wide reception area or footprint. Any properly tuned receiver located in the footprint can receive the signal. Newer technology will reduce the delay problem. A communication using satellite technology should be considered susceptible to interception.

Global mobile telephones using satellite technology have dropped dramatically in price. A handheld model with a satellite antenna built into the lid currently costs about \$500, whereas in 1993, it cost \$20,000. Such phones can be compatible with existing cellular networks and switch back and forth depending on the availability of cellular service.

Systems that use GEO satellites and a global network of earth stations support television, digital voice, fax, data, and email. These satellites maintain a fixed position at a nominal altitude of 22,300 miles (36,000 km) above the surface of the earth.

Medium earth orbit (MEO) satellite systems use satellites 6,500 miles (10,300 km) above the earth. The service is designed primarily for use by handheld, dual-mode telephones, which communicate with satellites and cellular systems, telephones in ships and aircraft, and fixed telephones in developing areas.

A system of 28 LEO satellites at an altitude of 480 miles (770 km) was designed to provide data message service for individuals and industries. Specific applications include monitoring of industrial installations and tracking of truck trailers and barges.

Handheld, dual-mode telephones, paging, and low-speed data and fax communications are the target markets for a system of 66 LEO satellites—at an altitude of 421 miles (675 km). Another system of 48 LEO satellites at an altitude of 763 miles (1,220 km) provides worldwide mobile and fixed telephone service.

A system of 840 LEO satellites has the characteristics of terrestrial optical fiber and coaxial cable networks. The low orbit—at 440 miles (700 km)—eliminates the signal delay of high-altitude satellites and accommodates delay-sensitive applications. The low orbit and high frequency transmission (30 GHz uplink and 20 GHz downlink) allows the use of small, low-power terminals and antennas.

Transportation companies in the United States and in developing areas have equipped trucks with two-way satellite messaging devices, which require the message for the vehicle to be typed. This system allows the vehicle operator to concentrate on driving and ensures message delivery if the vehicle is unoccupied. A global positioning system (GPS) feature of the service allows the home base to interrogate a transponder to determine the location of the vehicle at any time.

Wireless Interference

Proper signal reception depends on the ability of the equipment to discriminate wanted signals from unwanted signals and noise. Unwanted signals (interference) maybe encountered in any radio communication system. Some of the most common causes of interference are signals from other transmitters and industrial and atmospheric noise.

Regulatory authorities have adopted standards relating to frequency departure tolerances and maximum authorized power, but interference from other transmitters may be received because another transmitter frequency has been allowed to drift. Atmospheric conditions may allow interference from another station on the same frequency in a different part of the world.

Noise interference can be man-made or natural. Electrical transients radiating from circuits where electrical arcing occurs are the main sources of man-made noise. Such noise is caused by switches, motors, ignition and industrial precipitators, high-frequency heating, and other equipment. Man-made noise is a more serious problem for AM radio transmissions than FM. Use of FM is one way to avoid the noise problems. Noise from natural sources is characterized by static. A thunderstorm is an example of a natural phenomenon that would cause static. In video transmissions, noise manifests as a momentary breakup of the picture, lines or waves across the screen, or snow.

Facility construction also may affect radio and broadcast video reception. Heavy steel and concrete tend to limit the distance at which signals can be received, and dead spaces where no signals can be received are common. This problem often can be solved through the use of antennae, either connected to the receiving unit or radiating from a loop or leg strung throughout the structure.

7.3.3 **MICROWAVE TRANSMISSIONS**

A microwave transmitter operates at super high frequencies, between 30 and 300 billion Hz (30-300 GHz). It consists of a microwave generator, a power amplifier, a means of modulating the microwave carrier, and an antenna to transmit signals into the atmosphere. One-way and two-way communications are possible, and transmitting antennae also can be used for the reception of signals. Because of the frequencies used and the power levels needed, microwave installations often require FCC licenses. Microwaves penetrate rain, fog, and snow and are not affected by man-made noise. Microwave is used in television transmissions, multiplexed telephone signals, multiplexed alarm circuits, and high-speed data transfer.

Microwaves travel in a straight line. A transmitted beam striking a physical object is reflected, with a possible loss of energy depending on the shape, size, and reflective properties of the obstructing object. To circumvent obstructions, a passive reflector (a surface against which a microwave can be bounced like a billiard shot) is used. The reflector might be any flat surface, such as the side of a building or a specially designed metal plate. Another microwave station also might be used as a repeater at a third point, with common visibility to the two points between which communications must be set up. A repeater also can be used to extend the range of the microwave system. The same hardware is used in a repeater as in a terminal.

Where short distances are involved, microwave can be cost-effective in electronic protection systems. The entire microwave transmitter can be connected to an outside antenna with a low-voltage power cord and a cable to carry the signals. No conduit or elaborate installation is required. At the receiving end, a metal reflector or antenna is installed to collect the signals being directed to it. The receiver is connected to the antenna with a power cord and a cable to bring the signal into the termination point.

7.3.4 **LASER COMMUNICATION**

Laser is an acronym for “light amplification by stimulated emission of radiation.” The light from a laser is coherent (tightly focused in one direction) and can be modulated to carry signals, as radio waves do. The laser beam is modulated by passing it through a crystal. An electric field applied to the crystal modulates the polarization of the laser’s monochromatic light beam. A conventional audio, video, or data signal is applied to the electronic circuit of the transmitter, changing the electric field, which causes the crystal to rotate the axis of the laser beam to vary the amount of transmitted light. The laser beam is made to blink at an extremely high rate; the rate of blinking corresponds to the information in the signal being transmitted.

At the receiver, the laser beam is focused on a photo-detector that demodulates or recovers the electric field changes that were applied to the crystal by following the rapid changes in the intensity of laser light. The electrical signal from the photo-detector is then converted to conventional audio or video signals by an electronic circuit in the receiver. It is virtually impossible to intercept the beam without detection.

Line-of-sight transmission is necessary, and communication up to 4 miles (6.4 km) is possible without repeaters. If line-of-sight is not possible, the laser beam may be reflected off a mirror or mirrors, but each reflection reduces resolution quality. Snow, fog, and rain interfere with the beam, but the beam can be expanded to overcome such interferences. It is not necessary to obtain the approval of the FCC for such an installation.

7.3.5 **INTERCONNECTION**

The FCC has ruled that private communications systems may be interconnected with the public telephone network, provided the equipment is safely compatible with the telephone network equipment. The equipment must comply with Part 68 of the FCC rules to assure compatibility.

When connecting such equipment, users are required to notify the telephone company of the FCC registration number and a ringer equivalency rating on the equipment.

7.4 COMMUNICATIONS SECURITY

7.4.1 LINE PROTECTION

The switched telephone network, dedicated telephone lines, or proprietary circuits may be used in a protection system. To protect the communications, outside wiring should be installed underground and inside wiring should be installed in conduits. The telecommunications service provider should be requested to provide an underground service connection. In particularly vulnerable situations, the underground service should not be taken from the nearest utility pole, but from a more distant one to obscure the wire path.

Both local and long-distance telecommunications service are open to competition. While the major telecommunications provider networks are highly reliable, several large-scale network outages have occurred. The reliability of any proposed telecommunications provider should be assessed in detail. Dividing communications requirements between two providers will give a measure of assurance that communications can be maintained.

Line Supervision

A wire alarm system should be designed with line supervision to check the circuits automatically and immediately signal line faults. The simplest line supervision is an end-of-line resistor installed to introduce a constant, measurable electrical current. A variance from the normal level beyond a determined threshold will be detected and generate an alarm. This simple type of line supervision normally detects an open circuit (broken connection), a ground, or a wire-to-wire short. An attempt to intercept or defeat the circuit usually will cause a variance from the base circuit value and be detected. Tampering using methods that have little effect on the circuit value will not be detected if only basic line supervision is employed.

Where the value of the assets being protected or the information being transmitted is high, other methods of line security may be required, such as these:

- minimizing the permissible variance in circuit value
- using quasi-random pulses, which must be recognized by the control equipment
- using shifts in the transmission frequency

An analog communication is a mere audio reproduction of the source signal, whether human voice, musical instrument, or other tone. Anyone with access to the transmission line could overhear an intelligible transmission. This led to the development of certain devices designed to modify the intelligibility of the spoken message.

In a digital environment, the analog voice message is converted to a string of binary digits (zeros and ones). Access to the transmission link yields only the string of bits, which is not immediately intelligible. A recording of the communication could be made and the tape converted to analog format on appropriate equipment; however, the message content could also be encrypted.

7.4.2 **SCRAMBLERS**

Communications transmitted over copper wire in the telephone network can be intercepted at any point in the circuit. A scrambler is a tool for disguising information so that it is unintelligible to those who are eavesdropping. A number of different types of scramblers have been developed. The type of scrambler selected depends on the importance of the information to be transmitted and the skill of those who might intercept it.

Voice has two characteristics that may be modified to reduce or destroy its intelligibility—frequency (the pitch of the voice) and amplitude (its loudness). Scramblers invariably distort the frequency content of the voice.

Frequency Inverters

The simplest scramblers are known as frequency inverters. They operate by inverting the frequency content of the voice (Figure 7-5). Their major advantage is low cost and tolerance for poor communication channel conditions. However, the scrambled voice can be understood by a trained listener. They are inherently a single-code device and can, therefore, be broken by any listener with a similar scrambler or equivalent.

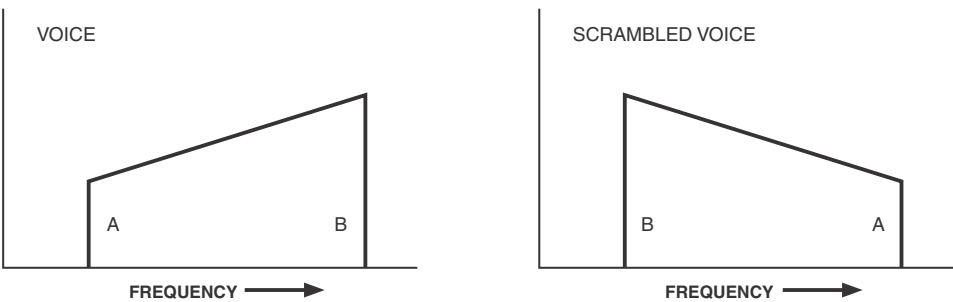


Figure 7-5
Frequency Inverter

Bandsplitters

Bandsplitters are extensions of the frequency inverter, in which the single speech band is broken up into a number of smaller frequency bands. These bands are inverted and interchanged prior to transmission (Figure 7-6). A five-band bandsplitter theoretically may scramble the frequency bands in exactly 3,080 different ways, of which 90 percent provide no better security than a frequency inverter. A trained listener can obtain a surprising amount of information by listening to the scrambled transmission.

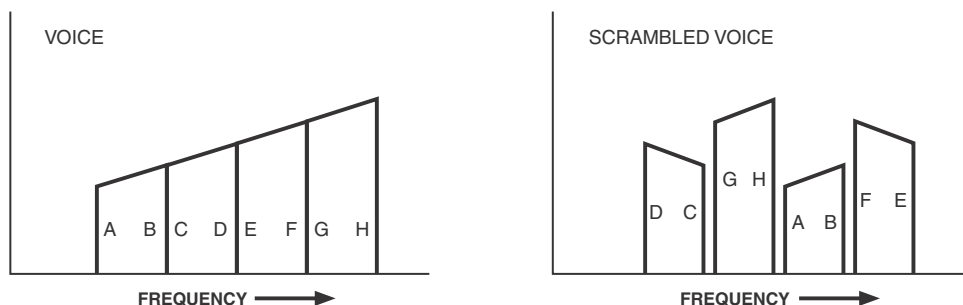


Figure 7-6
Bandsplitter

Rolling Bandsplitters

Bandsplitters may be improved by continuously modifying the way the frequency bands are interchanged, in accordance with a predetermined pattern. This scrambler is very similar to a simple bandsplitter. However, it cannot normally be broken on a trial-and-error basis by simply running through the available combinations of band interchanges. Still, a trained listener can obtain some information by listening to the scrambled transmission.

Frequency or Phase Modulators

Frequency modulator scramblers cause the voice spectrum to be inverted and continuously changed in frequency in accordance with a predetermined pattern. Phase modulators operate in a similar manner, but it is the phase rather than the frequency of the voice wave that is changed. These devices are similar to a rolling bandsplitter but usually have a higher level of security since the pattern can be changed more frequently. A trained listener may still obtain some intelligence from the scrambled transmission.

Masking

Masking is a technique for modifying the amplitude of the voice by adding another signal into the voice band. This masking signal is removed at the receiving unit to restore the original voice. The mask may be a single tone, a combination of switched tones, or RF noise. This is a very effective technique for destroying some syllabic content of the voice. Used alone, its security is not very good because a clear voice can be read through the mask fairly easily. Used in conjunction with a bandsplitter or frequency or phase modulator, masking provides a high degree of security.

Rolling Codes

Rolling bandsplitters, frequency and phase modulators, and many masked voice scramblers require the scrambled format to be changed periodically in a predetermined manner, usually at speeds between 100 times per second and once per 10 seconds. The electronic control signals that change the scrambled format are called the key-stream. Ideally, the key-stream should be completely random to prevent a code breaker from duplicating it. As the decoding scrambler has to be able to reproduce an identical key-stream, the key-stream has to be predetermined.

Key-streams normally have a fixed pattern length, then repeat the same pattern as often as required. The pattern length is typically between 15 bits and several billion bits. On first consideration, it would appear to be expensive and difficult to generate the longer key-streams, but this is not necessary, thanks to the use of an electronic device known as a pseudo-random generator. This device consists of an electronic shift register with appropriately connected feedback. When correctly set up, it generates a key-stream 2^{N-1} bits long (where N is the number of stages in the shift register). For example, a 23-stage shift register can generate a key-stream 8,388,607 bits long, which repeats every 9.7 days when switched 10 times per second.

A second feature of the pseudo-random generator is that it has a large number of connection configurations that enable it to generate maximum-length, totally different key-streams. The 23-stage shift-register has 364,722 different connection configurations or codes. A scrambler is unable to decode a transmission from another scrambler programmed with different codes.

All scramblers degrade the voice quality of a communications link. This is a particular problem when the performance of the link is degraded, and higher security scramblers require higher performance from the basic communication link than that required by lower security units. A digitized communication can be encrypted by any data encryption method. A high-speed computer processing the enciphering will produce a real-time communication in which the presence of the countermeasures will not be apparent to the parties to the conversation.

7.5 **ALARM CONTROL AND DISPLAY**

The AC&D system's control and display subsystem provides information to a security operator and enables him or her to enter commands affecting the operation of the AC&D system. The subsystem's goal is to support the rapid evaluation of alarms.

The alarm display equipment (the operator's console) receives information from alarm sensors. Several concerns must be addressed in console design:

- what information is shown to the operator
- how it is presented
- how the operator communicates with the system
- how to arrange the equipment at the operator's workstation

An effective control and display subsystem presents information to an operator quickly and clearly. The subsystem also responds quickly to any operator commands. The display subsystem must not overwhelm operators with detail but should show only necessary information. Available control functions should be only those that are relevant in the context of the current display.

Several types of information can be presented to aid in zone security, such as these:

- zone status (access/secure/alarm/tamper)
- zone location
- alarm time
- special hazards or materials associated with the zone
- instructions for special actions
- telephone numbers of persons to call
- maps of the zone

It is also important to examine how the operator will be alerted to the fact that action is required—specifically considering the type of display equipment, the format, and other visual features of the information that is to be displayed, as well as the design of the input equipment.

7.5.1 **ERGONOMICS: HUMAN FACTORS**

The control and display subsystem should be designed to serve the human operator. Ensuring normal temperature, humidity, noise, and general comfort factors creates an environment suitable for operator effectiveness and reduces frustration and fatigue. Adjustable lighting lets operators set illumination levels as needed for good viewing of video monitors. The design of the console should make it easy for the system and the operators to exchange information, such as alarm reports, status indications, and commands. Data should be presented in a way that makes its interrelations clear, and the techniques for transferring information from human to machine should limit the opportunity for errors.

Thus, the work area design must consider these factors:

- what the operator needs to see: people, equipment, displays, and controls
- what the operator needs to hear: other operators, communications equipment, and warning indicators
- what the operator needs to reach and manipulate: hand or foot controls and communications equipment

The area around the operator consists of zones of varying accessibility and visibility. All displays should be roughly perpendicular to the operator's line of sight and should be easily visible from the normal working position. Indications and operator inputs need to be prioritized, the most important ones being placed in the primary interface area (Figure 7-7). Displays in the primary interface area should not require much eye or head movement from the operator's line of sight, so they should be within a 30-degree viewing cone.

Operational displays that are used often should be placed in the secondary area, where the operator may have to move his or her eyes but not head. Support displays used infrequently, such as backup system and power indicators, may be placed beyond the secondary area.

Because the operator is not always watching the display panel, audible signals are used to alert the operator to a significant change of status. Different pitches and volumes can be used to distinguish classes of alarms, such as security, safety, or maintenance. Computerized voice output may also be used. The number of different audible signals should be kept low. Signals must be distinguishable in the complex audible environment of an AC&D control room.

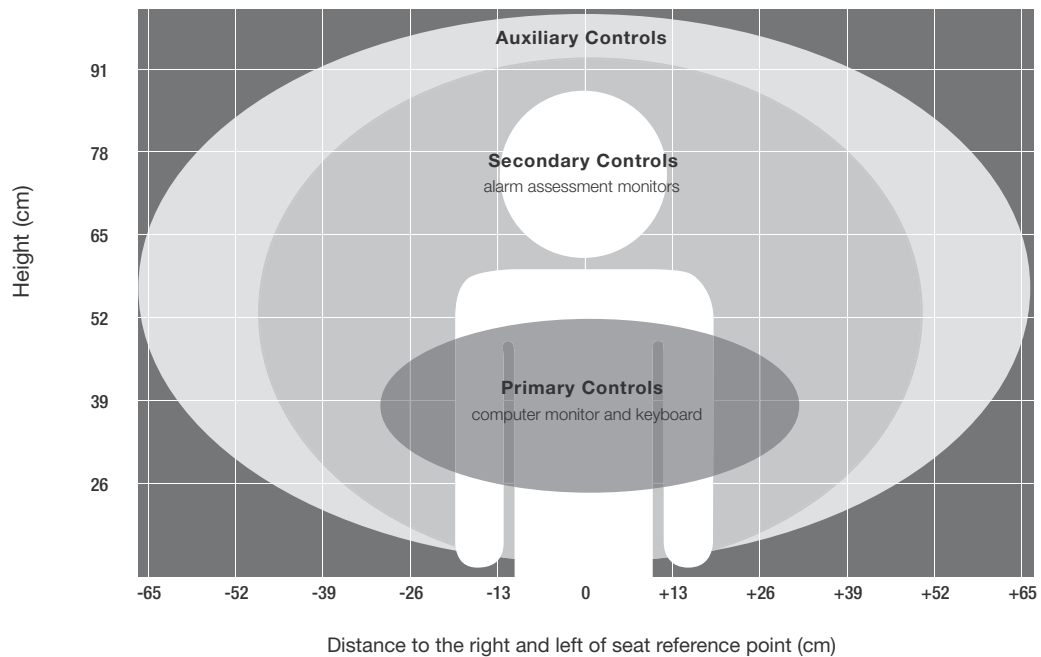


Figure 7-7
Placement of Operator Controls in an AC&D Console

Displays are usually installed in the center of the console, with readily identifiable controls placed on, below, or around the displays. Clarity is improved with neat labeling, color-coding, well-spaced grouping, and coding by shape. Place each control near the appropriate display reduces searching and eye movement. Touch panels that place controls on the display eliminate the need for many other control devices.

In addition to audible signals, system consoles should provide visual signals, such as flashing lights or blinking messages, to identify significant information. Colored lights or indicators can convey the status of alarms clearly. For example, traffic light colors (red, yellow, and green) are easily recognizable indicators for alarm/action, caution/abnormal, and proceed/normal, respectively.

The placement of support equipment depends on its importance and frequency of use. Communications equipment (microphones, telephones, additional CCTV monitors, and controls) must be given appropriate console space. Equipment that is not necessary for display and control functions should be placed outside the operator's immediate workspace. Installing computers and automatic control circuitry (such as CCTV switching equipment

and communication electronics other than microphones and controls) in a separate room offers several advantages. Maintenance personnel will have more space in which to work on the equipment, operators will not be disturbed by maintenance, and noise distraction, such as that from fans, is reduced. The equipment can be better secured against tampering, and environment conditions that are appropriate for the equipment can be maintained. For example, equipment may have cooling and humidity requirements that would not be comfortable for operators.

If more than one person at a time will operate the console, the operator/equipment interrelationships must be considered. Essential equipment should be duplicated for each operator, but operators can share access to secondary or infrequently used equipment.

7.5.2 **ERGONOMICS: GRAPHICAL DISPLAYS**

Well-designed graphical user interfaces (GUIs) can improve the display of security alarm information, and poorly designed GUIs can quickly overwhelm an operator. Various types of graphical information can be displayed on a computer monitor, subject to guidelines on how to best display that information.

A good graphical annunciator has a limited number of features. Current GUIs provide a wealth of features for displaying information, but a good display limits the ways information is displayed and which operations are allowed.

An on-screen display window may present text, graphics, or controls. It can be any size, and up to three windows can be displayed at once. One should be the full size of the screen and should contain an overview of the system status. Another, smaller window should present subordinate information as needed. Subordinate windows should be no larger than half the screen. A third window may display menus or other operational controls. Limiting the number and size of windows helps operators find important information quickly. Operators should not have to resize or move windows to view information.

Menus are typically displayed along the top of a window and can be nested, whereby selecting an item causes a subordinate menu to be displayed. Menus organize system commands clearly and concisely, and their structure should not be overcomplicated. A good menu contains no more than nine items and three levels. (Users may get lost in deeply nested menus.) A short menu reduces the time required to find a particular item. Complicated menu structures intimidate new users and annoy experienced operators.

Common commands should not be placed in menus but should be available as buttons. An on-screen button is like a push-button switch. Only commands that are valid in the current

context should be available. Sensor or map icons can be made to act as buttons, and buttons can be grouped into button bars, which group buttons for ease of access. Visible buttons should be limited to nine. Buttons should provide text labels that indicate their function.

GUIs can also display maps or graphics of the secured area. Maps quickly show the location of a security alarm. Maps may be scanned copies of paper media or electronically created graphics. The best graphics are stylized drawings that leave out excessive details. Displays typically require small-scale maps of about 1:5000. Maps provided for annunciation should be interactive, showing sensors on the map and providing mechanisms for the operator to display and control those sensors by performing operations on the graphic.

Sensor icons should use consistent graphics, sizes, and colors. When possible, sensors should be displayed together as a single icon to reduce screen clutter. No map should contain more than 50 sensor or group icons. Grouped sensor icons should indicate the state of the worst-case sensor in the group. For example, if one sensor in the group is in alarm, the group icon should indicate an alarm.

Text display is also needed. Dedicated areas of the display can provide descriptions of sensors. Only vital information should be displayed; details can be placed in subordinate windows. A good system also provides quick help.

Color can highlight important information but should be used sparingly. A user should not have to depend on colors to operate a system, as some 10 percent of the population has some degree of color blindness. No more than seven colors should be used. Menus, buttons, and backgrounds should be in consistent shades, often gray. Maps should be black-and-white or use low-saturation colors. Red, yellow, and green should be reserved to indicate sensor status.

The overriding design philosophy is “operator first.” Designers should follow these rules:

- The number of actions required to perform a command should be minimized. For a major command, an operator should only have to click the mouse once or depress a single key.
- Only operations that are valid in the current context should be available. For example, the operator should not be able to access a sensor if it is already accessed.
- The system should guide the operator through complex operations. Context-based command selection can direct operators’ actions without removing their control.
- Annunciator systems should not override operations in progress. If the user is assessing an alarm, the system should not replace the current information with notice of a new alarm. The assessment should continue while a nonintrusive notification of the new

event takes place. The operator can then decide whether to abort the current operation.

- Systems should not be annoying and should avoid loud, continuous alarms or bright, flashing displays.
- A given command should be performable in several ways. Making commands available as menu items, buttons, and keystrokes creates a friendlier system, enabling users to select their preferred methods.

An AC&D system exists to enhance site security. If it fails in its security task, it fails as a system. Elaborate graphics cannot save an ineffective system. A system that is easy to use is much more likely to succeed than an unnecessarily complex one.

7.6 SUMMARY

This chapter described the assessment of alarms through the use of a video subsystem and the alarm monitoring system. Assessment and surveillance are not the same. An assessment system associates immediate image capture with a sensor alarm to determine the response. Surveillance systems collect video information without associated sensors.

A video alarm assessment system consists of cameras at assessment areas, display monitors at the local end, and various transmission, switching, and recording systems. The major components include the following:

- camera and lens to convert an optical image of the physical scene into an electrical signal
- lighting system to illuminate the alarm location evenly with enough intensity for the camera and lens
- transmission system to connect the remote cameras to the local video monitors
- video switching equipment to connect video signals from multiple cameras to monitors and video recorders
- video recording system to produce a record of an event
- video monitors to convert an electrical signal to a visual scene
- video controller to interface between the alarm sensor system and the alarm assessment system

The level of resolution required in the video subsystem depends on the expected threat, expected tactics, the asset to be protected, and the way the video information will be used. Alarm assessment system performance must support protection system objectives. The alarm assessment subsystem must be designed as a component of the intrusion detection system. Interactions between the video system, intrusion sensors, and display system must also be considered.

The alarm communication and display system is a key element in the successful and timely response to a threat. The system controls the flow of information from sensors to the operator and displays this information quickly and clearly. The alarm communication and display system collects alarm data, presents information to a security operator, and enables the operator to enter commands to control the system. The goal of the display system is to promote the rapid evaluation of alarms. This chapter also discussed communication, control and display devices, equipment placement, the assessment system interface, and operator loading.

CHAPTER 8

ENTRY CONTROL

An entry control subsystem allows the movement of authorized personnel and material into and out of facilities, while detecting and possibly delaying movement of unauthorized personnel and contraband. Entry control elements may be found at a facility boundary or perimeter, such as at vehicle gates, building entry points, or doors into rooms or other special areas within a building. The entry control subsystem is a part of the detection function.

The objectives of an entry control system used for physical protection are as follows:

- to permit only authorized persons to enter and exit
- to detect and prevent the entry or exit of contraband material (weapons, explosives, unauthorized tools, or critical assets)
- to provide information to security personnel to facilitate assessment and response

Entry control refers to the physical equipment used to control the movement of people or material into an area. *Access control* refers to the process of managing databases or other records and determining the parameters of authorized entry, such as who or what will be granted access, when they may enter, and where access will occur. The terms are often used interchangeably in industry; however, there are advantages to differentiating between them. Many industrial access control systems include software to manage the database of those having authorized access, as well as the physical means of restricting entry or exit. Because the technical issues associated with the installation and use of entry control hardware are different than the administrative controls required to manage authorized access, they require separate consideration in order to achieve an effective and integrated subsystem.

The performance measures of entry control subsystems include throughput and error rates. Throughput is a measure of the time it takes for an authorized person or material to successfully pass an entry or exit point. Technology components that require longer throughput times may not be applicable in all situations, such as entry to an industrial facility at shift changes. Error rates will be discussed in more detail in the section below titled “Personnel Identity Verification (Biometrics).”

8.1 PERSONNEL ENTRY CONTROL

Personnel entry control is the portion of an entry control system used to authorize entry and to verify the authorization of personnel seeking entry to a controlled area. This verification decision is usually based on determining whether the person (1) is carrying a valid credential, (2) knows a valid personal identification number, or (3) possesses the proper unique physical characteristic that matches the person’s characteristic recorded at enrollment (biometrics, such as fingerprint, hand geometry, etc.). These three concepts are summarized as what you have, what you know, and what you are. With the exception of biometric devices, entry control devices may be used independently of the authorized person. A physical characteristic match will verify the person’s identity; a credential or an ID number only verifies that the person requesting entry has a valid credential or knows a valid number. Combinations of entry control technology can be used effectively to protect access to a facility. These combinations may reduce throughput but will make the system harder to defeat. Methods of personnel entry authorization include personal identification number, credentials, and positive personnel identity verification or biometrics.

8.1.1 PERSONAL IDENTIFICATION NUMBER

Some systems rely on a memorized number, referred to as a personal identification number (PIN). To gain entry the user enters the PIN on a keypad. Some systems use a coded credential to locate the reference file associated with that badge number in the access control database. In that case, an individual requesting access first inserts the coded credential and then enters a memorized number via a keypad. This number is compared to the one stored in the reference file for that person. If the numbers are the same, the person is granted entry. The memorized number may be selected by the individual enrolling, or it may be assigned. A four- to six-digit number is commonly used. This simple method does have weaknesses: (1) an individual could pass the PIN and credential to an unauthorized individual; (2) the PIN could be observed surreptitiously by an adversary (shoulder surfing); or (3) the PIN could be obtained by coercion. In addition, people often write PINs down, making it easier for an adversary to obtain them.

There are two primary considerations for selecting a secure PIN. The PIN should be long enough, and it should not be a number that is too meaningful to the individual to whom it is assigned. The PIN must have enough digits to prevent easy guesses. This is especially important where a PIN is the only criterion for granting entry. For a population of a few hundred, a four-digit PIN should be sufficient. Four digits allow for a total of 10,000 combinations, which is much larger than the number of people in the population. The probability of guessing a correct PIN is low under such circumstances.

If a person is allowed to choose a own PIN, he or she should not choose birthdates, partial social security numbers, phone numbers, or other numbers that may be easy for an adversary to guess. Other easy numbers, like 1-1-1-1 or 1-2-3-4, should also be avoided.

Some systems provide a maximum number of PIN entry attempts before disallowing the credential or generating an alarm to the central control system. Using the PIN in combination with credentials and biometrics helps raise the level of security.

8.1.2 **TOKENS**

Many types of tokens (also called credentials) are used in personnel entry control. They include the following:

- photo identification badge
- exchange badge
- stored-image badge
- coded credential

The first three require a manual check by a guard with a high degree of vigilance. Coded credentials are checked automatically.

8.1.3 **PHOTO IDENTIFICATION BADGE**

The photo identification badge is a common credential used for personnel entry control, but it is not always effective. A false photo identification badge can be made, or an individual can make up his or her face to match the face on a stolen badge. Also, because this kind of badge is manually checked, guard inattentiveness can reduce its effectiveness, especially at times when large numbers of people are entering a facility.

Exchange Badge

A badge exchange system requires that matching badges be held at each entry control point. When an employee presents a badge and requests entry, a guard compares the individual to

the photo on the corresponding exchange badge held at the entry control point. If the two match, the guard exchanges the badges and allows entry. The exchange badge may contain more information than the employee badge, and may be a different color. The employee's badge is held at the entry control point until the employee leaves the area, at which time the badges are again exchanged. In this way, the exchanged badge worn within the secure area is never allowed to leave the area. This reduces the possibility of a facility badge being counterfeited, lost, or stolen. The badge exchange system does not prevent someone from making up his or her face to match the image on a stolen badge.

Stored-Image Badge

The use of a stored-image (video comparator) system requires a guard to verify an individual's identity based on visual characteristics. A securely stored image is used for comparison with a real-time image of the individual requesting entry.

Two of the most important features of such a system are enrollment capability and access time. Enrollment capability is the maximum number of images that can be stored by the system. The access time is the time required from entry of the identification number until the stored image is displayed for viewing. These systems use a coded badge or keyboard to find the stored image for display and visual comparison by the guard.

Stored-image systems are not based on a unique, measurable characteristic, such as a fingerprint, so they are not considered to be personnel identity verification. However, they have an advantage over manual photo identification systems in that it is difficult to tamper with the stored image. In this way, stored-image systems are comparable to badge exchange systems. Nonetheless, they are still susceptible to the use of makeup to disguise an unauthorized person.

8.1.4 CODED CREDENTIAL

Coded credential systems, also called key-card systems, are commercially available with a wide range of capabilities, including these:

- maintenance of entry authorization records for each coded credential
- provision of unique identification code numbers that can be read by a machine
- termination of entry authorization for an individual without the need to recover the person's badge or credential
- provision for several levels of entry authorization, such as entry only at selected entry control points or only at certain times of day

Entry authorization records can be updated each time entry is requested using a coded credential. Each entry action and its time of occurrence, entry location, and the coded credential identification number can be recorded and listed on request. Many coded credentials are in the form of a badge that is worn or carried while in a facility. Wright (1988) provides a technical introduction to the use and application of coded credentials.

Many techniques are available for coding a badge. The most common techniques include magnetic stripe, wiegand wire, bar codes, proximity, and smart cards.

Magnetic stripe encoding is widely used in commercial credit card systems. A strip of magnetic material located along one edge of the badge is encoded with data. These data are then read as the magnetic strip is moved through a slotted magnetic reader. The measure of the resistance of a magnetic material to changes in the stored information when exposed to magnetic field is called its coercivity. The coercivity is defined as the magnetic intensity of an applied field required to change the information. The unit of magnetic intensity used to describe the coercivity is the oersted.

Two materials have been used as the magnetic stripe medium. The one most commonly used for credit cards is a 300 oersted (low-coercivity) magnetic material. This material is relatively easy to erase. The coercivity of the second magnetic stripe material is in the range of 2,500 to 4,000 oersteds (high-coercivity). This material is the one most commonly used in security credential applications and is very unlikely to be accidentally erased. Common household magnets are not strong enough to erase high-coercivity stripes. Less common rare-earth magnets, on the other hand, do produce field strengths strong enough to alter high-coercivity magnetic stripes.

The use of alphanumeric encoding allows both the badge-holder's name and a badge number to be included. Credential forgery is relatively easy since data from the magnetic strip can be decoded or duplicate badges encoded by the use of commercially available equipment. This vulnerability can be mitigated to a great degree through the use of proprietary, nonstandard encoding and reading techniques. The use of proprietary systems, however, may limit the ability to interface with other equipment or subsystems. This may also limit choices when considering upgrades or expansions.

Wiegand wire technology has been in existence for some time, and the wiegand signal output format has become a de facto industry standard. While this technology is not used much anymore, the wiegand data protocol is still in common use.

The bar code, widely used in retail trade to automatically identify products at the point of sale, is sometimes used on coded credentials. The varying widths of the bars and spaces between them establish the code. To read the card, an optical sensor scans the bar code and

transmits the information to a decoding unit. Typically, the bar code is printed on the credential and is used in much the same way as a magnetic stripe. Unless the bar code is covered with an opaque covering, it is relatively easy to duplicate. This opaque covering is becoming more commonplace as the bar code badge moves into the security credential market. Two-dimensional symbologies (2-D bar codes) are also used on security credentials and are capable of storing more information than their one-dimensional counterparts.

The proximity badge is one whose information can be read without the badge being physically placed into a reader device. Proximity badges can be classified by the method of powering the badge, operating frequency range of the badge, and read-only or read/write capability (Wright, 1987).

The electronic proximity identification badge, a small RF transponder/transmitter, must be powered in some way. A long-life battery packaged with the unit powers active badges. For some types of badges the battery power is applied only when the badge enters the interrogation field. For others, the badge continuously broadcasts and the reader antenna picks up the RF data as the badge enters the reading field. The passive badge draws its power from the reader unit through the RF signal as it enters the interrogation field.

Proximity badges fall into two groups according to frequency. Low-frequency badges are in the 125 kHz range, and high-frequency badges range from 2.5 MHz to over 1 GHz. A read-only badge contains a specific code that is usually fixed at the time of manufacture and cannot be changed. The read/write badge, on the other hand, usually contains a larger data field than read-only badges and can be programmed by the system manager as required.

A smart card is the size of a standard bank credit card with an integrated circuit embedded in the card. Gold contacts on the surface of the card allow for communication with a reading device. Contactless smart cards use RF communications to talk to the reader and do not have the gold contacts. Cards with only memory circuits serve much the same function as magnetic stripe cards: badge number, user's name, and other information can be stored and read. A true smart card includes a microprocessor that makes the card smart and sets it apart from memory cards. The size of memory on the smart card ranges from 8 kilobytes to 64 kilobytes, with projections of 1 megabyte available in the future.

The main advantages of the smart card are its large memory and its high degree of resistance to forgery or compromise. These advantages must be considered relative to the high cost of smart cards. Many smart cards have the ability to encrypt communications, which adds another level of protection. When facility populations are large and the security level is not extremely high, the cost of smart cards is prohibitive. However, issuing smart cards to a small population for use at a very high-security facility or to limit access to certain areas in large facilities may be appropriate. Examples of the latter case might be entry into areas

containing precious metals or executive suites. A facility may also have extensive administrative concerns such as training, health care records, or property control; a smart card that combines one or all of these record-keeping functions with security features could be cost-effective.

Homeland Defense Presidential Directive 12 (HSPD12) is a presidential directive signed by President George W. Bush in August 2004 that directs the entire federal government and all contract agencies to use a single, high-security credential. The credential is based on Federal Information Processing Standard 201 (FIPS 201) and uses both contact and contactless smart card technology. The implementation of this new credential is ongoing. This directive primarily affects federal and federal contractor facilities but may also have some impact on private industry. For example, personnel driving vehicles into federal or contractor facilities on a routine basis may be required to obtain a federal ID. Oversight for the development and testing of the credentials and related equipment (readers and entry control systems), as well as issuance procedures, is being provided by the General Services Administration (GSA) and the National Institute of Standards and Technology (NIST). If a company is required to comply with the directive, the details must be worked out on a case-by-case basis with the government. Considerable information can be obtained by conducting an Internet search on HSPD-12 or FIPS 201. Caution must be used when reviewing information obtained through a Web search because a considerable number of vendor sites will appear in the search results. Some vendors state that their products are HSPD-12 compliant but do not mention certification. Compliance may simply mean that the vendor believes the product meets all the requirements, whereas to be certified the product must be submitted to GSA and NIST for testing. Upon successful completion of the testing, the product will be placed on the government's official approved products list, which can be found at <http://fips201ep.cio.gov/apl.php>.

8.1.5 **PERSONNEL IDENTITY VERIFICATION (BIOMETRICS)**

Personnel identity verification systems corroborate claimed identities on the basis of one or more unique physical biometric characteristics of the individual. Commercial equipment is available that uses hand or finger geometry, handwriting, eye pattern, fingerprints, speech, face, and various other physical characteristics. All personnel identity verification systems consider the uniqueness of the feature used for identification, the variability of the characteristic, and the difficulty of implementing the system that processes the characteristic.

Biometric devices can differentiate between verification and recognition. In verification mode, a person initiates a claim of identity, presents the specific biometric feature for authorization, and the equipment agrees. In recognition mode, the person does not initiate

the claim; the biometric device attempts to identify the person, and if the biometric information agrees with the database, entry is allowed.

Many biometric technologies use error rates as a performance indicator of the system. A Type I error, also called a false reject, is the improper rejection of a valid user. A Type II error, or a false accept, is the improper acceptance of an unauthorized person. Often these error curves are combined and displayed graphically to show the equal error rate. This is the crossover point where Type I errors equal Type II errors. This point is not necessarily the point at which the device should be operated. The equal error rate does not occur at the point where Type I or Type II errors are both lowest. However, the figure may be useful when comparing various biometric devices.

When selecting or deploying biometric devices, consideration of the security objectives is required to ensure that the device will operate as required. Some systems may be set to operate in an area where the device will minimize false rejects, whereas others may minimize false accepts. The device cannot minimize both error types simultaneously, so a decision must be made as to the balance between false accept and false reject rates. This has a significant implication for system operation. A low false-accept rate compromises system security, but allows all authorized users entry. False rejects, on the other hand, can deny access to authorized users to maintain high security. The security manager will undoubtedly hear about the cases of false rejects, particularly if senior managers or other influential employees are denied access. Adversaries, on the other hand, are unlikely to report that entry was obtained due to false acceptance.

Hand/Finger Geometry

Personnel identity verification using the hand geometry system is based on characterizing the shape of the hand. The underlying technique measures three-dimensional features of the hand, such as the widths and lengths of fingers and the thickness of the hand.

The hand-read sequence is initiated by presenting a coded credential or entering a PIN. The user then places the hand on a reflective platen; the device has guide pins to help the user properly align the fingers. Although the guide-pin arrangement is best suited to the scanning of right hands, the left hand can be enrolled and scanned by placing the left hand on the platen palm up. A solid-state camera takes a picture of the hand, which includes a side view for hand thickness. Due to the combination of infrared illumination and the reflective platen, the image of the hand appears as a silhouette to the camera. The system measures the necessary lengths and widths and creates a representation of the hand called a feature vector.

During verification, the feature vector is compared with previous measurements (the template) obtained during enrollment. If the feature vector and template match within an allowable tolerance, verification is successful. Testing of a hand geometry system at Sandia

National Laboratories indicates that Type I and Type II error rates of less than 1 percent are achievable (Holmes, Wright, & Maxwell, 1991). Ruehle and Ahrens (1997) prepared a report on the use of a hand geometry unit in an operational environment.

A similar system uses two fingers to verify identity. This two-finger geometry system measures finger lengths and widths of the index/middle finger pair. Because only one guide pin is used (between the two fingers), the left- or right-hand fingers work equally well. The functional concept of this device is similar to the hand geometry system.

Handwriting

Signature verification has been used for many years by the banking industry, although signatures are easily forged. Automatic handwriting verification systems have been developed that use handwriting dynamics, such as displacement, velocity, and acceleration. Statistical evaluation of these data indicates that an individual's signature is unique and reasonably consistent from one signature to the next. Transducers that measure these characteristics can be located in either the writing instrument or tablet. These systems provide low security and are best used in applications where signatures are already used to authorize transactions.

Fingerprints

Fingerprints have been used as a personnel identifier for more than 100 years and are still considered one of the most reliable means of distinguishing one individual from another. The art of processing human fingerprints for identification has been greatly improved in recent years by the development of automated systems. Such systems, which rely on image processing and pattern recognition, have application in personnel entry control. Many commercial systems now available perform fingerprint verification.

Most fingerprint verification systems use minutia points, the fingerprint ridge endings and bifurcations, as the identifying features of the fingerprint, although some systems use the whole image for comparison purposes. All fingerprint identification systems require care in finger positioning and accurate print analysis and comparison for reliable identification.

Optical methods using a prism and a solid-state camera are most often used to capture the fingerprint image. Dry or worn fingerprints can be difficult to image using optical methods, so special coatings have been applied to the optical platens to enhance the image quality. The purpose of these coatings is to ensure a good optical coupling between the platen and fingerprint.

Ultrasound is another fingerprint imaging method. Because it can image below the top skin surface to the lower layers where the fingerprint is not damaged, it is not as susceptible to dry

or worn fingerprints. Due to the raster scan required by the ultrasonic transducer, ultrasound imaging is not as fast as optical methods.

Direct imaging sensors that use solid-state devices are also available for acquiring fingerprint images. Capacitive, electric field, and thermal methods have been commercially developed. It is thought that the projected lower cost of these devices, due to the efficient manufacture of silicon chips, will make fingerprint verification devices common on the desktop for secure computer log-on. Overcoming the difficulties of hardening delicate silicon chips for everyday use has delayed their widespread implementation. Electrostatic discharge, finger oil, and sweat are harsh on silicon devices.

Eye Pattern

Another technology uses the iris to accomplish identification. The iris is the colored portion of the eye that limits the amount of light allowed into the eye. This system uses a video camera to image the iris structure of the eye. The unique structure of an iris can be used to identify an individual. This system operates in the recognition mode, so entry of a PIN is not required. A distinct advantage of this system is that the camera images the iris at a distance of about 10-12 in. (25-30 cm), so no physical contact between the face and the scanner is required. In addition, the eye is externally illuminated with visible light so there is no LED shining in through the lens.

Data from a laboratory test of a prototype iris scanner indicated some difficulty with glare off glasses. This caused some Type I (false reject) errors. No Type II (false accept) errors were observed in the laboratory test (Bouchier, Ahrens, & Wells, 1996). Later devices incorporated glare detection and compensation features to counteract problems. Transaction times range from 4 or 5 seconds (by practiced users) up to 15 seconds (for those new to the system). Approximately 2 percent of the population cannot be enrolled due to blindness or other iris damage, extremely dilated eyes, or very dark irises, so they require another method of granting secure access.

Voice

Voice is a useful attribute for identity verification and is appropriate for automatic data processing. Speech measurements useful for speaker discrimination include waveform envelope, voice pitch period, relative amplitude spectrum, and resonant frequencies of the vocal tract. The system may ask the user to speak a specific, predetermined word or to repeat a series of words or numbers selected by the system to verify access.

While this technology currently offers low security, it is an attractive alternative due to its ease of deployment and acceptance by the public. Voice recognition systems need only be installed on one end of a telephone system, and perhaps centrally located, reducing the

number of units required. In addition, most people have experience with using telephones, so training is minimal, and distrust of the technology is low. As a result, units are currently being marketed for security applications, and further development is active.

Voice systems also have some associated procedural issues. A person's voice can change due to sickness or stress, so a procedure or backup method of access must be provided to accommodate these instances.

Face

Facial verification systems use distinguishing characteristics of the face to verify a person's identity. Most systems capture the image of the face using a video camera, although one system captures a thermal image using an infrared imager. Distinguishing features are extracted from the image and compared with previously stored features. If the two match within a specified tolerance, positive identity verification results.

Although facial systems have been proposed and studied for a number of years, commercial systems have only been available recently. Developers have had to contend with two difficult problems: (1) wide variations in the presentation of the face (head tilt and rotation, presence or absence of glasses, facial hair changes, facial expression changes, etc.), and (2) lighting variations (day versus night, location A versus location B, etc.). Performance of currently available face systems has not yet approached that of more mature biometric technologies, but face technology does have the appeal of noncontact, and the potential to provide face-in-the-crowd identifications for identifying known or wanted criminals. This latter application could be useful in casinos, shopping malls, or other places where large crowds gather. This technology is used successfully in some situations but has been removed after several years of disappointing results in other applications. Thorough testing under the environments this device will be used under is recommended before implementation at a site.

Other Techniques

Keystroke technology (typing patterns) has been developed and marketed for secure computer log-on. Other verifier techniques based on such things as ear shape, gait (walking patterns), fingernail bed, and body odor have been studied, but little development has been attempted.

Because each biometric technology has some limits in terms of inability to enroll certain people, procedures dealing with this event must be developed. Examples include very dry or heavily damaged skin and nonrepeatable signatures and speech patterns. In addition, authorized users may occasionally suffer injuries such as broken fingers or hands, eye injuries or surgery, or other medical conditions, which may temporarily affect their ability to use a biometric device. Additional technology or security officer intervention may be

required to address this problem. Jain, Bolle, and Pankanti (1999) have written a thorough review of biometric techniques and their application. Others (Rejman-Greene, 1998) have discussed biometric devices and security considerations.

8.1.6 **PERSONNEL ENTRY CONTROL BYPASS**

When coded credentials or biometric technologies are used to allow personnel access into rooms, the use of keyed locks as a bypass route should be considered. This bypass will be useful in case of a component or power failure. The possible vulnerability introduced by this alternate access path can be countered through the use of a door sensor. If the door is opened, an alarm will be recorded and can be investigated. This will happen whether a key is used or if the lock is picked or broken. For areas or rooms where multiple entry doors exist, only one door need be equipped with a keyed lock.

8.2 **CONTRABAND DETECTION**

Any item that is prohibited from an area is contraband. Contraband screening typically occurs when entering a secure area. Unauthorized weapons, explosives, and tools are contraband because they can be used to steal or to gain access to or damage vital equipment. Drugs, cell phones, radios, computers, and computer media are some additional items that could be considered contraband at a facility. Where these items are a part of the threat definition, all personnel, materials, and vehicles should be examined for contraband before entry is allowed. Methods to screen for weapons, tools, and explosives are discussed in the following sections. The technologies discussed include manual search for all threats; metal detectors for weapons, tools, and bomb components; package searches (X-ray systems) for weapons, tools, and bomb components; and explosives detectors for bulk explosive charges and trace explosive residues. Additionally, there is a brief discussion on the role of chemical and biological agent detection in facility protection.

8.2.1 **MANUAL SEARCH**

Manual search should not be overlooked as a contraband detection method. Screeners performing manual searches can be very effective if they are properly trained to recognize the threat items and if they remain vigilant. Advantages of manual searches are low hardware investment cost and flexibility. Two disadvantages, compared to the technologies described below, are slow throughput and higher labor costs.

8.2.2 METAL DETECTORS

One system employed for the detection of metal is a magnetometer. The magnetometer is a passive device that monitors the earth's magnetic field and detects changes to that field caused by the presence of ferromagnetic materials. This method detects only ferromagnetic materials (those that are attracted by a magnet). Materials such as copper, aluminum, and zinc are not detected. While most firearms are made of steel, some are not and therefore will not be detected by a magnetometer. Although magnetometers have not been used for contraband screening for many years, research and development of a modern magnetometer has been conducted in recent years. Although the term *magnetometer* is often used to refer to metal detectors in general, this device differs greatly from modern active metal detectors and its continued use is discouraged.

Most metal detectors currently in use to detect contraband carried by personnel actively generate a varying magnetic field over a short period. These devices either detect the changes made to the field due to the introduction of metal to the field, or detect the presence of eddy currents that exist in a metallic object caused by a pulsed field. The magnitude of the metal detector's response to metallic objects is determined by several factors, including the conductivity of the metal, the magnetic properties of the metal (relative permeability), object shape and size, and the orientation of the object within the magnetic field.

At present two methods can be used to actively detect metal: continuous wave and pulsed field. Continuous-wave detectors (no longer commercially available) generate a steady-state magnetic field within the frequency band of 100 Hz to 25 kHz. Pulsed-field detectors generate fixed frequency pulses in the 400 to 500 pulse-per-second range.

A steady-state sinusoidal signal is applied to the transmitter coil located at one side of the detector arch. This coil produces a magnetic field of low strength. The receiver coils are mounted on the opposite side of the arch such that a person being screened passes between the transmitter and the receiver coils. The signal is detected by the receiver coils and is then routed to a balanced differential amplifier, which amplifies only the difference between two signals. When there is no metal present within the arch, there is no difference in the signals at the inputs to the differential amplifier; therefore, there is no output signal from the amplifier. When a metallic object enters the arch, the changes it makes to the magnetic field disturb the balance of the receiver coils. The unbalanced field produces a difference at the differential amplifier resulting in an output signal. This signal is then further amplified and phase-checked. If the signal exceeds a selected threshold, an alarm is generated. The phase detection permits some optimization of detection for either ferromagnetic (high relative permeability) or nonferromagnetic (low relative permeability) metals.

The coil arrangement is similar to that of the continuous-wave metal detector. The greatest difference is that the balanced receiver coils are not required for pulsed-field operation. The

multiple transmitter coils produce magnetic field flux patterns that lessen the effects of object orientation on detector response. The low inductance transmitter coils are driven with a series of pulses that produce short bursts of magnetic field (as short as 50 microseconds), 200 to 400 times per second. During the time that the magnetic field is present, the receiver amplifiers are switched off. Following the end of the transmitted pulse, the receiver amplifiers are switched on for a period, typically a few tens of milliseconds. When there is no metal present in the arch, the output of the receiver amplifiers is the low background electromagnetic noise. When there is a metallic object present in the arch, the collapse of the magnetic pulse induces an eddy current in the metal. This eddy current decreases rapidly as a function of the resistivity of the metal but persists long enough to be present when the receiver amplifiers are switched on. The signal is then further amplified and phase-detected. If the signal exceeds a selected threshold, an alarm is generated. The phase detection again allows for optimization for detection of ferromagnetic metals or nonferromagnetic metals. Modern digital technology allows for more analysis of the signal, resulting in better discrimination between different types of metals and real targets and the harmless metallic objects carried by people being screened.

When a portal metal detector is used to detect very small quantities of metal such as gold, detection may be very difficult. In the case of a continuous-wave detector, the use of a higher-than-usual frequency will enhance detection; in all cases very-high-sensitivity operation will be required. Because high-sensitivity operation will sharply increase the nuisance alarm rate, an area for personnel to change out of steel-toed shoes and to remove other metallic items from their body may be required. Handheld metal detectors can detect even very small quantities of metals and may be better suited to the task of screening for very small items. The disadvantage of handheld metal detectors is the requirement for active guard participation in the screening process and the time required for the search. Handheld metal detectors can also be considered intrusive due to the proximity of the metal detector to the person being screened. This can be especially intrusive when the screener and the person being screened are of opposite sex. Many sites, notably airports, provide same-sex operators to address this unease.

Because the magnetic field is not confined to the area between the coils and metal detectors are sensitive to metal moving outside the physical boundaries of the detector, care must be exercised in determining detector placement. Any movable metallic objects either in front or to the side of the detector, such as doors, forklifts, and carts, can cause nuisance alarms. Electromagnetic transients, such as radio transmitters, power-line fluctuations, and flickering fluorescent lighting, can cause false alarms.

Metal detectors are designed to be tolerant of some nonmoving metal in their immediate area. Reinforcing steel in concrete floors and walls and other metallic building materials can be tolerated to some degree; however, installing a metal detector against a steel support

beam is not recommended. Large quantities of metal can cause severe distortions in the magnetic field. In some cases the metal detector will not operate and may generate an error alarm; in other cases the detector may continue to operate but have areas of extremely low or high sensitivity. These distortions may lead to missed targets or unusually high nuisance alarms due to innocuous items. Metallic items, such as safety equipment, metal trash cans, chairs, and other items, may not completely interfere with a metal detector if placed close to the detector but can cause distortions to the detection field. For this reason, some installations institute a no-move rule for these metallic items within the vicinity of the detector following installation testing.

8.2.3 PACKAGE SEARCH

Packages may be searched for contraband manually or by active interrogation. Active interrogation methods used to detect contraband objects include a family of X-ray approaches: single energy transmission X-ray, multiple-energy X-ray, computed tomography (CT) scan, and backscatter X-ray. In general, these methods are not safe for use on personnel; however, a backscatter X-ray technology for screening personnel will be discussed in the next section. Simple single-energy-transmission X-ray imagers are used to find metallic items (e.g., weapons, tools, and metal components in bombs) and the other techniques are designed to image materials with low atomic numbers. The atomic number (Z) is the number of protons in the nucleus of an atom. Examples of low- Z contraband materials are explosives, drugs, and some foods. Low- Z atoms include hydrogen, oxygen, carbon, and all the elements up to aluminum, which is Z number 26.

A conventional single-energy-transmission X-ray package search system produces an image for an operator to inspect. This approach is effective when the operator is properly trained and vigilant, and when the image is not too cluttered. Metals strongly attenuate X-rays, while less dense and low- Z materials do not. Conventional X-rays will not penetrate the heavy materials sometimes used for shipping containers or in vehicles. Higher-energy X-rays or multiple-energy X-rays can be used to assess the contents of the larger and denser shipping containers and vehicles. Because most of the development of low- Z screening devices is directed toward the detection of explosives, these technologies are discussed in detail below. While discussion of these devices is focused on explosive detection, most of these technologies can be adjusted to search for drugs as well.

Explosives Detection

Explosives detection technologies are divided into bulk and trace methods. This division is based on the target of the technology—macroscopic (bulk), detonable amounts of explosives, or the particle and vapor (trace) residues associated with handling explosives. Bulk technologies have the advantage of targeting specific threat amounts of explosives.

Trace techniques target residue that can lead a screener to perform secondary screening. Usually, the bulk techniques use ionizing radiation that is not suitable for use on people due to safety considerations. Methods of bulk explosives detection and trace explosives detection are presented in the following sections. References on explosives detection include an excellent description of various technologies (Yinon, 1999), a survey of commercially available equipment (Theisen et al., 2004), and a survey of existing and potential standoff technologies (National Academy of Sciences, 2004).

Bulk Explosives Detection

Bulk explosives detection technologies measure characteristics of bulk materials, thereby screening for the presence of explosives. Some of the bulk characteristics that may be measured are the X-ray absorption coefficient, the X-ray backscatter coefficient, the dielectric constant, gamma or neutron interaction, and microwave or infrared emissions. Further analysis of these parameters can result in calculated mass, density, nitrogen, carbon, and oxygen content, and effective atomic number (effective Z). While none of these characteristics are unique to explosives, they are sufficiently unique to indicate a high probability of the presence of explosives. Fortunately, many materials that share similar bulk characteristics with explosives are not common among everyday items. Some bulk detection devices are sensitive enough (minimum detectable amount is less than the threat mass) and are specific enough (low nuisance alarm rate) to allow for effective automated detection of explosives. Automated detection provides significant advantages, including reduced labor costs and lower reliance on human interpretation of images for detection.

X-ray technologies are continuing to grow more sophisticated, and are widely deployed in many configurations from portable package imagers to very large systems capable of imaging a large truck and its cargo. Using backscatter technologies, people can be safely imaged, although X-ray technologies are most commonly used for package searches. These devices usually serve a dual purpose. The package being searched for guns or other contraband is simultaneously analyzed for the presence of explosives.

Simple, single-energy-transmission X-ray scanners do not provide enough information for an explosives search, so a method to extract more information is needed. Dual-energy technologies measure the mass absorption coefficient and enable approximation of the effective Z-number. The image displayed can be highlighted using colors to draw the operator's attention to areas of the image with a low Z-number that matches explosives. Backscatter technology can image low- Z using the relatively large amount of X-ray energy scattered back in the direction of the source by low-Z materials. These areas appear bright in the backscatter image, drawing the operator's attention.

Computed tomography (CT) is an automated technology for explosives detection that provides detection of small threat masses. The X-ray source and detectors are mounted on a gantry that spins around the package, imaging the contents from many different angles. A computer uses that data to construct a three-dimensional representation of the contents. CT scanners are the only X-ray approach that can extract enough information to calculate the material's mass, density, and mass absorption coefficient. This extracted information can be used for automated detection of materials that may constitute a threat. Compared to simple transmission X-ray devices, CT devices have significantly higher purchase and maintenance costs due to the heavy spinning gantry. CT also suffers from relatively high nuisance alarm rates (up to 20 percent) compared to trace technologies, mainly from foods and some polymers.

For vehicle and cargo-container searches, high-energy X-ray devices are available. Often these devices are large and built into fixed sites, even into their own buildings, for screening commercial cargo shipments. The high-energy illumination is highly penetrating, allowing a reasonable image to be produced through the engine compartment or the filled trailer of a commercial truck. The method for producing the high energy light is immaterial. Gamma-ray devices that use a radioactive source instead of an X-ray tube are also used for this purpose. Backscatter X-ray technology may be combined with high-energy technology to provide low-Z detection.

Low-dose backscatter X-ray devices can safely examine people for hidden items, providing an image of the body beneath the clothes. A person entering a scanner booth must be scanned two times, front and back, to ensure that no explosives are secreted on the person. The radiation dose to a person being screened is about 10 microrem. This low dose meets the NRC requirement that personnel must not receive a radiation dose above 100 millirem/year (10 CFR Part 20, Section 20.1301 (a) (1), 1991). Radiation exposure should always be kept as low as reasonably achievable (10 CFR Part 20, Section 20.1301 (d) (3), 1991).

Nuclear technologies interrogate a vehicle (or package) using gamma rays or neutrons. Gamma ray devices are similar to high-energy X-ray devices discussed above. Thermal neutron activation (TNA) devices determine the nitrogen content of a material. A thermal (low energy or slow) neutron is absorbed by the nucleus of nitrogen-14, producing excited nitrogen-15. This excited atom radiates a gamma ray of specific wavelength, and detection of this specific gamma ray is evidence of nitrogen content. Because many explosives are nitrogen-rich, these devices can automatically detect their presence. Both the neutrons and the gamma rays are very penetrating, making them suitable for large, dense item searches. Pulsed fast neutron absorption (PFNA) can determine carbon and oxygen content. Here, "fast" means high energy (several MeV). International law prohibits the irradiation of food with energies above 10 milli-electron volts (MeV) due to concerns of making the food radioactive, so there is a potential risk if a system using more than 10MeV is used to screen

food shipments. When combined with TNA, a PFNA device can also measure nitrogen content. In theory, measuring carbon, nitrogen, and oxygen content allows more specific identification of explosives and better rejection of nuisance materials (that may be nitrogen rich). The major drawbacks of these devices are their cost (for vehicles, \$500,000 and up, though TNA is less expensive), size, throughput, and use of radioactive materials in the neutron source or neutron generator tube. Some small TNA package search systems (under 100 lb. (45 kg)) are commercially available.

Quadrupole resonance (QR) technology is a promising commercial technology that uses pulsed low-energy radio waves to determine the presence of nitrogen-rich materials. QR is very sensitive (detects small threat masses) for some explosives. Contraband can be shielded from the radio interrogation with a thin covering of metal, but the device can detect the presence of the shielding and warn the operator. A QR scanner is compact, relatively low-cost (about \$100,000), and does not subject the package to ionizing radiation. Handheld QR systems are in development and may provide a useful tool for manually screening people for explosives.

Raman analysis uses laser interrogation followed by analysis of the spectrum of scattered light to identify materials. Portable, lightweight systems have been developed for hazardous materials detection, including explosives. A laser can shine through some containers (such as glass) or directly on the suspect material surface. Small but visible amounts of material are required for detection. As currently configured, this new technology could be useful for screening through bottles or plastic bags, but it is not appropriate for package searches.

Technologies for standoff detection of explosives are in great demand because of the need to detect explosive devices from a safe distance. But at present, standoff detection remains an area of much research and few commercial products, which is especially true for the detection of suicide bombers and large vehicle bombs. Infrared cameras can be used to image people for concealed objects that could be explosives. Passive and active millimeter-wave (approximately 100 GHz, sometimes called terahertz or THz) imaging systems are available that operate like infrared systems but in a different part of the frequency spectrum. Laser methods that look for characteristic fluorescence or atomic emission are another example of techniques under development. Standoff detection of explosives is a difficult challenge. Vendor claims regarding the performance of standoff detection devices should be investigated to verify their performance against the defined threat in the expected environment.

All the bulk explosives detection technologies have strengths and weaknesses. A successful system based on bulk detection techniques may consist of a combination of two or more technologies. If enough information is gathered on a suspect material through the combination, a real determination of the presence of explosives may be made.

Trace Explosives Detection

Use of trace explosives detectors has become common for checkpoint screening in the last decade. Trace vapors and microscopic particles are associated with explosives and their handling. Detection technologies for trace explosives include ion mobility spectrometry, colorimetry, chemiluminescence, mass spectrometry, fluorescence, and canine olfaction. Key performance metrics for trace detectors include limit of detection (the smallest detectable amount) and selectivity (ability to distinguish one material from another). Many trace detectors are amazingly sensitive, detecting less than a nanogram. Still, vendor claims regarding detector performance should be verified before purchase. True detection of explosives traces leads a screener to search further for the materials in the threat definition.

Sampling is a key part of effective trace detection because the trace residues must be collected and then delivered to a detector for analysis. Swipe sampling, where a fabric swab is rubbed across the object (e.g., person, package, or vehicle), is the most efficient method of collecting particle residues from hard surfaces and produces the most collected mass for analysis. The collected sample on the swab is vaporized by heating and directed into a detector. Vapor sampling, where the air next to the object is collected (often with some agitation), is most efficient for sampling from inside containers or from soft surfaces. Because it does not require touching the object, vapor sampling is less invasive than swipe sampling.

The challenge involved in detecting trace explosives vapors is evident after consideration of the low-vapor-phase concentrations of several common high explosives. Concentrations in the parts-per-billion or parts-per-trillion range are typical, with further reductions in vapor pressures encountered when the explosive constituent is packaged in an oil-based gel or solvent (for example, RDX in C-4 plastic explosive). Explosive molecules also readily adsorb upon most materials at room temperature, and decompose upon moderate heating or upon exposure to large doses of energy; hence, transport and collection of vapor-phase explosive molecules is achieved only at the expense of significant sample loss.

In an ion mobility spectrometer, or IMS, the analyte molecules in an air sample are negatively ionized using a radioactive Ni-63 source and chloride dopant, then passed into a drift cell through a shutter, which opens periodically (about every 20 milliseconds). Within the drift region, the ionized species move down an electric field gradient against a counter-flow of an inert gas. The ions separate by mobility, with the lightweight species and their smaller cross-sections progressing more quickly upstream than the larger species. At the end of the drift region, the ions strike a Faraday plate that records the output voltage as a function of ion drift time. A typical IMS drift cell is about 5 cm in length with an electric field gradient of 200 V/cm. Under these conditions, the drift times of the explosives molecules range from 5 to 15 milliseconds. While common high explosives form negative ions, some of the emerging explosives threats like triacetone triperoxide (or TATP) also form positive ions.

IMS instruments with both positive and negative ion analysis capability are now commercially available.

IMS-based detectors provide high sensitivity (nanogram quantities) to dynamite, military-grade TNT, and plastic explosives compounds, at instrument costs of \$40,000 for bench-top models, or \$25,000 for handheld units. The combination of selective ionization and time-of-flight separation achieved in the drift region provides enough specificity for screening applications. Interferents and nuisance alarm rates are low in the field, with some exceptions such as compounds used as fragrances in lotions and perfumes. Sensitivity, ease of operation, instrument robustness, and low maintenance are advantages of IMS. Although their purchase cost is lower, the handheld detectors have higher maintenance requirements and need AC power for operation beyond a few hours.

Several vendors offer technologies where a color change is evidence of explosive presence. Generally these kits have some materials like a spray, test paper, or ampoule that gets consumed during the test. Chemical reactions produce the color changes. Frequently, multiple solutions are used in sequence to determine what explosive (if any) is present. The great advantage of this method is low cost and portability. Disadvantages include high nuisance alarm rate and disposal of consumable chemicals. Some have a strong smell.

Chemiluminescence detectors use photochemical detection. The vapor sample is collected and separated into its components using a fast gas chromatograph. The sample is then heated so that any nitrogen compounds present will decompose to form nitrogen oxide (NO). Reaction of NO with ozone forms an excited state of nitrogen dioxide (NO₂), which emits a photon that can be detected using a phototube. The coupling of the photoemission and the chromatograph permits identification of nitro-based explosive compounds. Without the gas chromatography step, one would only know that a nitrogen-containing material was present. With the chromatographic separation, identification of several explosives in a single sample is possible in under a minute.

Chemiluminescence detectors have excellent sensitivity (picogram quantities) to common high explosives, including compounds with very low vapor pressures such as RDX and PETN. However, chemiluminescence instruments are also the most expensive of the commercial detectors, have the longest analysis time, and require more maintenance than other trace detectors.

It is possible to place another detector after the chromatography step, for example, an electron capture detector. Electron capture detectors, or ECDs, take advantage of the high electron affinity of nitro compounds to identify trace explosives in a vapor sample. Electron capture technology itself cannot determine the specific explosive detected, but by coupling the ECD with another technology such as a gas chromatograph (GC), the type of explosive

can be identified. GC/ECD is more commonly used for laboratory analysis than for routine checkpoint screening. Advantages of GC/ECD are low cost, good specificity, and low limits of detection. Disadvantages are long analysis times (minutes are typical) and frequent GC column maintenance.

In mass spectrometry, ions are processed in magnetic and electric fields to determine their mass-to-charge ratio. Quadrupole mass spectrometry and quadrupole ion trap time of flight are two examples of this method. A wide variety of mass spectrometer configurations are available.

In a quadrupole mass spectrometer, the sample molecules are negatively ionized with an electrical discharge, accelerated in an electric field, and then focused onto an ion detector with the magnetic field of a quadrupole. Selected mass numbers characteristic of explosives can be monitored individually or a range scanned continuously. The mass of the parent ion and characteristic fragment or daughter ions can be determined. Alarms are produced when a threshold current is exceeded for a given mass number or combination of mass numbers.

A quadrupole ion trap time-of-flight mass spectrometer collects ions in the trap, where they orbit. Periodically the trap is emptied and the time for the ions to travel to the detector is measured. The time-of-flight depends on the square root of the mass (kinetic energy) of the ion. IMS is similar to time-of-flight mass spectrometry, except IMS occurs at atmospheric pressure and mass spectrometry occurs under vacuum. Alarms are produced from the mass spectrum in the same way as described above.

Mass spectrometry is the gold standard of the analytical chemistry laboratory. Advantages of mass spectrometry are specificity and low limits of detection. These devices can be easily reprogrammed to detect additional analytes, a desirable feature in a world of evolving threats. However, high costs, high maintenance requirements, and the need for expert operators have slowed the deployment of mass spectrometers for routine screening. Newly developed instruments are better suited to explosives detection in checkpoint settings, and improvements continue.

Amplifying fluorescent polymers can change their fluorescence in the presence of some explosives. Systems have been developed with a fluorescence that quenches in the presence of an explosive molecule like TNT. The TNT molecule quenches the fluorescence of all the monomers (thousands of them per molecule), thus amplifying the effect many times. Highly sensitive detection of low picogram to femtogram quantities is possible. The polymers are coated onto capillary tubes and placed adjacent to a photomultiplier tube. Vapors are drawn through the tube, and changes in the fluorescence above a threshold produce an alarm. Advantages of these systems are small size, low cost, and high sensitivity. Not all explosives

will produce a response with the existing polymers, and research to develop coatings for more explosives is ongoing.

Canine olfaction (smelling by dogs) is used widely in law enforcement and the military for locating hidden explosives and drugs. Where mobility is required, such as building searches or quickly relocating detection capabilities, canines excel. Detection is actually made by the handler who observes the dog behavior. Canines and their handlers require constant retraining to continue to identify synthetic compounds such as explosives. Moreover, the reliability of canine inspection is subject to the vigilance and skill of the handler and the health and disposition of the dog. Canine teams also require frequent breaks, which may create the need for multiple teams. While acquisition costs are low, the labor of the handler is a recurring cost. As a result, the use of canines is less common at fixed checkpoints, where commercial explosive detectors are gaining greater acceptance as the preferred method for screening.

Trace explosives detection portals have been developed over the past decade, and are now deployed at many airports. A trace portal collects particle and vapor samples from a person after agitating the person's clothing with short bursts of air. These pulses of air help dislodge explosives residues, while the air surrounding the person is filtered. The filter collects explosives vapors and particles for several seconds, and then the filter is heated to desorb any collected explosives into a trace detector (ion mobility spectrometer or mass spectrometer). Screening time ranges from 10 to 25 seconds. Advantages include automated detection, high sensitivity (nanograms), and noninvasive screening of the whole person. Disadvantages are size, cost (approximately \$150,000), and maintenance. For comparison, swipe sampling of a person is possible, but would likely be considered invasive, and would require more than a minute per person.

A summary of many commercial explosives detectors is available (Theisen, 2004). Commercial trace explosives detectors must be carefully selected to meet the needs of each facility. Vendor claims should always be verified through testing in the appropriate operating environment. The sensitivity, nuisance alarm resistance, response time, operating and maintenance costs, and list of explosive materials in the threat definition are all factors to consider when selecting a detector.

Chemical and Biological Agent Detection

Chemical and biological agent detection is typically performed with point sensors, searching for evidence of an attack at the site perimeter. In the case of chemical agent attack, an adversary may attack suddenly with large (and therefore quickly lethal) concentrations, and the security system goal is an early warning for successful interruption and neutralization of the adversary. Military and environmental chemical (trace) detectors have been developed

over the past century for this purpose. Some modifications may need to be made if continuous operation over extended time periods is required. Careful consideration should be made regarding nuisance alarm rates. Because the response to a chemical attack must be fast and complete, nuisance alarms or drills may not be tolerated well by those required to respond. Chemical detectors normally sample air at various perimeter locations and may not be appropriate for use in checkpoint screening. Some chemical sensors use optical methods to achieve standoff detection.

Biological agent detection differs from chemical detection in two ways. First, most biological agents are not immediately lethal, so response time may not be as critical as for chemical attacks. Second, detection methods usually involve filtering air for several hours and then analyzing the filter (several more hours). As a result of this delay, it can be difficult to detect the biological agent in time to prevent exposure; however, once the agent is identified any personnel who have been exposed can be treated. As a result of this limitation, biological detection is a very active area of research at present. Other materials that cross the site perimeter, such as water (via rain, streams, piped potable water) and air (pollen, pollutants), can also be monitored, but these are usually considered part of environmental monitoring, not contraband detection.

8.3 LOCKS

Locks are important elements in the entry control system of a facility since they secure the movable portions of barriers. However, locks should generally not be relied upon as the only means of physical protection for important areas at a facility. Because an individual with enough skill and time can compromise them, locks should be used with complementary protection measures, such as periodic guard checks and sensors.

The lock is the most widely used method of controlling physical access. Locks are used for homes, vehicles, offices, hotels, safes, desks, cabinets, files, briefcases, display cases and jewelry boxes. Locks are among the oldest of security devices and have amassed a slew of technical jargon to define the locksmith's craft.

Locks can be divided into two very general classes: 1) those that operate on purely mechanical principles; and 2) those that are electrical and combine electrical energy with mechanical operations and are commonly associated with automated access control systems.

8.3.1 **MECHANICAL LOCKS**

A mechanical lock uses a barrier arrangement of physical parts to prevent the opening of a bolt or latch. In such a lock the functional assemblies of components are:

- The bolt or latch that actually holds the movable part (door, window, etc.) to the immovable part (jamb, frame, etc.);
- The keeper or strike into which the bolt or latch fits. The keeper is not an integral part of the lock mechanism but provides a secure housing for the bolt when in a locked position;
- The tumbler array that constitutes the barrier or labyrinth that must be passed to move the bolt; and
- The key or unlocking device, which is specifically designed to pass the barrier and operate the bolt.

In most mechanical locks, the bolt and barrier are in the permanently installed hardware or lockset; the key or unlocking device is separate. However, in some mechanical locks that use physical logic devices, the entire lock is a single assembly. Examples of these include locks with integral digital keypads that mechanically release the bolt if the correct sequence is entered, and dial-type combination locks.

Primary Types

The primary types of mechanical locks are as follows:

- **Warded lock.** The mechanical lock longest in use and first developed is the warded lock. The lock is exemplified by the open, see-through keyway and the long, barrel-like key. In the illustration, six different keys are shown plus a master or skeleton key that opens all six locks. Still found in older homes, farm buildings and older inns, the warded lock is a very simple device.

The greatest weaknesses of this type of lock are its vulnerability to spring manipulation by any key that is not stopped by the wards and corrosion due to weathering and age. A well-planned, modern locking program does not include warded locks. In any installation where extensive warded locks are already present, phased replacement or augmentation with other locks is recommended.

- **Lever lock.** A significant lock improvement after the warded lock came in the 18th century with the perfection of the lever principle. (A lever lock should not be confused with a lever handle on a lockset.) The lever tumblers are flat pieces of metal held to a common pivot and retained in place inside the lock case by the tension of spring wire. Each lever is cut on the edge opposite the pivot to accommodate a lug or appendage attached to the bolt and is designated as a fence. When all the levers are positioned so that the fence slides into the spaces cut into the levers, the bolt can be withdrawn.

The lever lock offers more security than the warded lock. Moreover, by placing two or more fence cuts on each lever tumbler, it is possible for two or more keys, cut to different dimensions, to operate the lock. This permits master keying, discussed later in this chapter.

The lever lock finds continued application today in such varying situations as desk, cabinet and locker installations, bank safe deposit boxes and U.S. mail boxes. Although the lever lock is inherently susceptible to picking, it can be designed to provide a high degree of lock security through resistance to picking.

- **Pin tumbler lock.** The most important development in the history of mechanical locks to date has been the invention of the pin tumbler in the 19th century by Linus Yale, an American who also developed the dial-type combination lock. The pin tumbler is probably the most widely used lock in the United States for applications such as exterior and interior building doors. A number of very useful refinements have been added to the basic pin tumbler in recent years so that now a very high level of lock security can be achieved with many models.

The pin tumbler consists of the same basic elements as all mechanical locks: the bolt moving device, the maze or labyrinth and the keyway. It is in the maze or obstacle segment that it differs.

A **conventional cylinder** always has its key pins equally spaced in one row only. When master keying is employed, split pins are introduced, and the number of key changes is greatly reduced. Conventional cylinders usually contain only five, six, or seven pins.

In a **high security cylinder**, the pins and driver are interlocked so that random movement of the pins by lock picks or keys not specifically coded for the lock will not properly align the pins and drivers. In this type of lock, the keys are cut at precise angles, as well as depths, so that when inserted into the plug the key will both raise the individual tumbler array of driver and pins to a shear line and, at the same time, turn each pin so that the interlocking mechanism is positioned to pass through a special groove at the base of the plug, thus permitting the entire plug to rotate enough to move the bolt. A variant of this principle is found in the Medeco high-security cylinder. In the Medeco lock, instead of grooves at the bottom of the plug through which the interlocking feature of the pins pass, a side bar is moved into a cutout housing in the shell or withdrawn into grooves in the pins. In both types of high-security locks, the keys are specially cut at specific angles, making routine duplication of keys quite difficult, except on special equipment used by the manufacturer.

- **Wafer tumbler lock.** A fairly late development, the wafer tumbler lock, utilizes flat tumblers fashioned of metal or other material to bind the plug to the shell. Their design permits master keying. In addition, wafer tumbler locks may be designed for double-bitted keys.
- **Dial combination locks.** Dial combination locks, while not employing a key, resemble the lever tumbler lock in many respects. They operate by aligning gates on tumblers to allow insertion of a fence in the bolt. However, the tumblers are fully circular and are interdependent; that is, moving one results in moving the others. This makes the order of movement important and is really why these are true combination locks rather than permutation locks.

With combination locks, the theoretical maximum number of combinations is the base number of positions on each tumbler (typically 100 on a good grade lock), raised to the power of the number of tumblers. Thus, a four-tumbler combination lock, each of whose tumblers had 100 numbers of dial positions, would have a theoretical maximum of 100^4 or 100,000,000 changes.

Electronic combination locks have been developed as replacements for dial combination locks on safes and secure document cabinets. These devices are powered by the user turning the dial; the combination numbers are displayed via an LCD rather than by gradations on the dial. The display is viewable only from a limited angle and the number being dialed bears no direct relationship to the position of the mechanical dial. Additional features include a time-out of a specified number of seconds between each number dialed, and a two-person rule where two numbers must be dialed before the lock will open. As each user is assigned an individual number, an audit trail of which combinations were used to open it and when it was opened is available. The lock can memorize the number of unsuccessful attempts to open. Because of the electronic precision of the system, there is no reduction in the number of combinations due to the unavailability of adjacent numbers. These locks are claimed to be immune from all the typical defeat modes of a regular mechanical combination lock as well as from electrical and magnetic attacks.

Master Keying

The principle of master keying is that a single lock may be operated by more than one key by designing various different keys to engage or work upon different tumblers or different aspects of the same tumblers. Master keying is utilized to provide a hierarchy of access to groups of locks, from access to only one lock through access to increasingly larger groups of locks, and, finally, to access to all locks in the population. Master keying is defended and advocated on the theory that in large locking programs involving hundreds or thousands of individual locks, it would be totally unworkable to require those persons with broad or

variable access requirements to carry a separate key for each lock. Thus, master groupings are developed within which a single key opens all the locks in that group.

Three major security difficulties are presented by the master keying technique and they must be balanced against the alleged need for the master key convenience.

First, very effective master key accountability must be maintained. The loss, compromise, or unauthorized use of such a key exposes all the locks in that group. Restricted access key cabinets and software running on personal computers are products that can assist the security professional in achieving adequate key accountability.

Second, in any manipulation of the lock, additional positions or possibilities are presented for surreptitious unlocking by the creation of multiple shear lines or gate openings.

Third, for cylinder locks the additional parts required in the lock core create the need for additional maintenance. In some types of master keyed mechanical locks there is frequent difficulty with locks binding or sticking because additional master key elements, often very frail, become disarranged or break and necessitate a mechanical disassembly and removal of the involved lock.

Security Vulnerabilities of Mechanical Locks

Mechanical locks are subject to a variety of attacks that can result in their failure or compromise. Some types of attack require a high level of skill, while others are almost invited by the mere appearance of the lock.

- **attack by force:** e.g., separating the door or movable element from the jamb or immovable element; removing the lock from its housing and exposing the bolt to manual manipulation; or snapping pin tumblers to turn the plug freely.
- **surreptitious attack:** e.g., picking with various tools
- **attack by impression-making and “try” keys:** If a blank designed for the particular keyway can be introduced into the lock before any biting cuts have been made, it may be possible, by applying turning pressure, to make faint marks on the key blank. “Try keys” or “jingle keys” as they are sometimes called, are key blanks that are correctly milled to fit the particular keyway and that contain random biting. Insertion in the keyway and combined turning/raking movements may cause the lock to open.

Rearranging Mechanical Locks

Periodically, an installed locking system requires changes in the lock tumbler arrangement because of changes in authorized personnel compromise of the system; loss or unaccount-

ability of keys or major changes in occupancy. There are several ways in which the tumbler change or the equivalent effect can be achieved. One is the simple relocation of the lock.

Door locks may be rotated among doors, cabinet locks among cabinets, and so forth. For security benefits to accrue from simple relocation, there should be no identification on the lock that would permit a former key holder (perhaps still in possession of the key) to recognize the lock in its new location.

The second and more effective way is to rearrange the actual tumblers within each lock to a new combination. With lever and wafer tumblers this means disassembly of the lock and a change in the order of the tumblers. The same tumblers, however, may be used many times in such changes. With pin tumbler locks the same thing can be done; that is, the same pins can be used but in different tumblers.

The convertible or interchangeable core is a design feature available from some manufacturers of pin tumbler locks that makes possible the very rapid redistribution of combinations. It can be replaced on the spot by another core already arranged to the desired new scheme.

8.3.2 **ELECTRIFIED LOCKING MECHANISMS**

Electrified locking mechanisms allow doors to be locked and unlocked by a remote device. The device may be a simple electric push button or a motion sensor, or may be a sophisticated automated access control device such as a card reader or digital keypad. In addition, many access control systems allow the use of Boolean logic to augment the control of electrified devices. Boolean logic lets you organize concepts together in sets. For example, Boolean logic relates to the combination of conditions; for example, “if door A is locked and door B is locked, then door C can be unlocked.”

This is useful in the design of mantraps and other high security operations. When considering failure and defeat mechanisms for locks, the addition of remote control devices requires that these other devices be included in the analysis.

Before describing the different types of electrified locking mechanisms, it’s useful to define two important terms clearly—fail safe and fail secure. These terms are usually applied in reference to fire/life safety codes and relate to doors in the path of egress from an occupied space that are required to be unlocked either at all times of occupancy or only during a detected fire emergency. Codes also state that the means of egress must be by a single action that requires no special knowledge although there are some exceptions for banks, jewelry stores and other high security applications. Turning a door handle or pushing an exit device (panic bar) are allowable single actions. Pressing a button, turning a key, using a card reader

or keying a number on a digital keypad before turning the handle do not constitute single actions. Local fire codes vary by municipality and the reader should refer to them when specifying any door locking mechanisms.

A fail safe locking mechanism is one that will unlock under any failure condition. The failure mode most commonly considered is loss of power, but failure of the mechanism itself and any connected control device need to be considered also. Most, but not all, locks related to code-required egress are fail safe to ensure that they provide free egress if a power failure occurs at the same time as a fire emergency. Note, however, that the lock for a door that normally provides free egress simply by turning a handle or depressing the exit bar from the secure side does not need to be fail safe. For example, an electrified exit device (panic bar) will mechanically unlock its door when pushed regardless of whether the lock is electrically energized or not.

A fail secure lock is one that will remain locked when power is lost or another failure occurs. As noted above, a fail secure lock may be used on a door in the path of egress provided that free egress is available regardless of the state of the lock's power or other control mechanisms.

Primary Types

The primary types of electrified locking mechanisms are as follows:

- **Electric deadbolt.** The electric deadbolt is the oldest and simplest of all electrical locking devices. A solenoid (electro-magnet) moves a deadbolt, typically mounted on a door frame, either into or out of a strike plate on a door. The mechanism can be either fail safe, automatically unlocking on the removal of power, or fail secure, remaining locked on the removal of power. The electric deadbolt is not normally recommended for application to doors required to be unlocked automatically in response to a fire alarm signal. This is because the bolt may bind in the strike plate if pressure is on the door when power is removed. This can occur in a panic situation when people are pressing on the door before the lock is de-energized. Some deadbolts are designed with tapered bolts to prevent binding but the reader should check with local building and fire codes before specifying this type of device for fire egress doors.
- **Electric latch.** Somewhat similar to an electric deadbolt is the electric latch. It is also solenoid activated, mounts on the door frame and uses a strike plate in the door. Instead of a deadbolt, a beveled latch is used. It has an advantage over the deadbolt because the latch does not need to be withdrawn for the door to close since it is pushed into the lock mechanism against spring pressure as it rides up and over the strike plate.
- **Electric strike.** The electric strike operates as an adjunct to any standard mechanical lock. The operating principle is simple: electrical energy is delivered to a solenoid that either opens or closes a mechanical latch keeper or strike plate. (Note that the electric

strike is not a lock but operates with a lock to hold the door closed or to permit it to be opened.) Such devices have been used for many years in apartment houses, business offices, commercial installations and occupancies in general.

A typical application of the electric strike is to control passage in one or both directions. The lockset handle is fixed (i.e., will not turn) on the side(s) from which passage is controlled. The only means of access becomes remote, unlocking the electric strike by a button or switch within the secure space, or by an automated access control device, such as a card reader or digital keypad. If the knob or handle on the secure side of the door remains operational (i.e., it will turn), then egress can be free. If the knob or handle is fixed on both sides, egress can be achieved by the same types of devices described for access. Additionally, if the mechanical lockset is equipped with a lock cylinder on one or both sides, the door can be unlocked with a key.

- **Electric lockset.** The electric lockset is simply a regular mortise lockset that has been electrified to control the ability to turn the handle. As the lock is contained within the door, the door must be drilled to allow power wiring to be fed to the hinge side. The cabling must then be fed either through or around the door hinge.

This type of electric lock is becoming increasingly popular for automated access control applications. The normally fixed, unsecure side handle of a storeroom function electric lockset is controlled by an access control device (e.g., a card reader) while the secure side handle remains operational at all times for unimpeded egress. Some models offer an option of a sensor switch in the lock that is activated when the inside handle is turned. This provides a request-for-exit signal to the access control system to automatically shunt any magnetic switch or local horn associated with the door so that alarms are not sounded for a valid egress. This option requires the specification of a four-wire (instead of two-wire) transfer hinge to accommodate both the lock power and the sensor switch cabling.

- **Exit device.** Also known as a panic bar or crash bar, the exit device is commonly used on doors in the path of egress from structures with high occupancy. The rim-mounted device requires little modification to the door, as it is surface mounted. The mortise-mounted device requires the locking mechanism to be mortised into the edge of the door in the same manner as a regular mortise lock. Vertical rod devices are used on doors with double leaves where there is no fixed frame or mullion to accept a latchbolt. The rods, which move into holes or strike plates in the frame header and floor to restrain the door, can be surface mounted or concealed within a hollow door.

Exit devices can be electrified to permit remotely controlled re-entry via a push button or card reader/keypad. One special application of this type of hardware is the delayed egress locking system. Developed as a compromise between safety and security, this system is usually applied to doors intended to be used only for emergency fire egress.

Instead of allowing immediate egress when pushed, activation of the bar starts a 15 or 30 second delay after which the door unlocks. Special signage is required to inform users of the delay; the system must be connected to the fire alarm system; and the delay must not occur in the event of a fire or other defined life safety emergency. Although it will not usually provide enough of a delay to permit interception of an escaping thief, the system will sound a local alarm and report that alarm condition to a central monitoring location. A CCTV camera can be used to identify the perpetrator and any articles being carried, and to record the incident.

- **Electromagnetic lock**, The electromagnetic lock, also known simply as a magnetic lock, utilizes an electromagnet and a metal armature or strike plate. When energized, the magnet exerts an attractive force upon the armature and thus holds the door closed. Although the lock is usually mounted at the head of the door, it can be mounted on the side. This location, while reducing the door passage width, provides a considerably more secure door.

Magnetic locks are rated by the pounds of force required to separate the armature or strike plate from the electromagnet, and are available from 500 to 2,000 lbs. Although most applications will need only a single magnetic lock installed on a door, multiple locks can be used for high security requirements.

A valuable feature of regular electromagnetic locks is that they involve no moving parts and are less maintenance sensitive than mechanical or electromechanical devices. As long as the surfaces of the magnets and the armature are kept clean and in alignment, and provided there is assured electrical power, the devices will operate as intended. Better electromagnetic locks have built-in switches to monitor the bonding of the magnet and armature and to monitor the door position. These sensors are important to void the simple defeat mechanism of placing a non-metallic sheet between the magnet and the strike to reduce the bonding power.

Electromagnetic locks are intrinsically fail-safe because removal of power releases the strike plate. In high security applications, back-up power should be used to ensure that the lock fulfills its function in the event of a power failure. It's possible to use electromagnetic and electric bolt or strike plate locks in combination. For example, consider an area under ingress and egress access control that must remain secure against unauthorized entry but permit free egress during a defined emergency.

These types of locks are also used in delayed egress systems as described above for egress devices. A switch in the magnet senses that the door has been pushed and starts the required countdown. The same caveats as described above should be observed.

8.3.3 **DESIGNING SECURE LOCKING SYSTEMS**

Despite the sophistication of modern access control systems, such as card and biometric readers authorizing access via computer software, the traditional mechanical lock and key remain the most commonly used system for restricting access to corporate or institutional facilities and assets. The justifications for this choice include low cost, simplicity of operation and reliability.

However, all of these benefits will be negated if the locking systems are not professionally planned and administered. The loss of a master key could require the replacement of all key cylinders within a facility at a cost of thousands of dollars. Similarly, the lack of control over key issuance and return could lead to asset losses from theft or destruction that could cost an organization millions of dollars.

Locking systems usually control the opening of a door or portal to an area, e.g., a building perimeter door; to a room, e.g., a confidential records storage room; or to a smaller container, e.g., a filing cabinet or a safe. Locking systems are also used to control usage of equipment, e.g., cashier operations, control of door operators, and to secure individual assets, e.g., cable locks on portable computer equipment. Each of these applications needs to be considered in the locking system plan.

Of equal importance in the design of protection measures is assessing the totality of the area, for example, the physical strength of all the barriers that could provide access to the space. The door and its frame—as well as the surrounding walls, the windows, the ceiling and the floor—also must be considered. An expensive lock on a hollow wooden door may deter the amateur but, other than leaving evidence of a break-in, will not stop a professional. Similarly, a strong metal door set in a weak frame that can be broken easily or surrounded by a wall of standard sheet rock construction, will not prevent access by a determined intruder—regardless of the strength or sophistication of the lock.

As with the planning and design of any security or protection system, the practitioner should first ask these questions:

1. What assets (people, structure, equipment, negotiables, operations, information, etc.) need to be protected and what is their value to the organization?
2. What are the threats to those assets and what are the probabilities of those threats occurring?
3. Who requires access to the assets and how often?
4. What level of system flexibility should be considered?

5. What impact will there be on regular operations by implementing controls?
6. What consideration should be given to the organization's culture or image?
7. Does the organization have the available staff resources and skills to plan, design, implement, operate and maintain the systems or will outsourcing of some, or all, of these functions be required?
8. What budget is available to implement the protection strategy and, often more important, what funds are available to operate and maintain the system?

The Design Plan

Locking systems are coordinated arrays of mutually supportive and complementary locking elements. They are based upon design plans which consider:

- the need for different, concurrent levels of security control for locked spaces;
- the likelihood that such levels will change with time;
- the probability that some (or many) users will require common access in some spaces and exclusive access in others;
- the possibility that access devices (keys, cards or tokens) may be lost, compromised or damaged; and
- the requirement that there be effective means for adapting the system to planned, as well as unanticipated changes.

A locking system must be designed, not simply installed. The difference between adding or removing locks within a facility purely on a "when needed" basis, and developing a locking concept which will permit changes in system size and changes in occupancy or use while retaining security control is important. Without lock planning, security will usually degrade to mere privacy. And unauthorized persons may gain access capability to secured spaces, or accountability for issued access devices may be lost, or the convenience of status level management may be sacrificed. If it is not clear who has access to what spaces, a locking program is not secure. If it is not possible to provide multiple levels of access, the program is not convenient. In either case, the program will also be uneconomical because it will not provide what is required, and any money spent on it will be misapplied.

The cautions and principles discussed here are directed toward making a locking system both secure and convenient, with due regard for the tension between those objectives. Greater convenience often means reduced security and enhanced security usually implies less convenience. A balance can be found, however, if the system needs are correctly defined at the beginning. That is one aspect of lock system planning—another is to select the most

appropriate locking mechanisms for the particular application. These may be conventional mechanical locks or electronic locks and may include codes and personal physiological characteristics. The planning considerations are common to all systems.

Lock System Planning Considerations

The following are common design or planning criteria and require systematic study before either the locking hardware or the scheme is finally decided upon:

- total number of locks
- major categories of sectors of the system
- security objectives
- size and turnover of population
- related or supportive security subsystems
- intelligence or information requirements
- criticality of asset exposure

Locking Policy

As with all major security functions, the lock program should be based upon a written policy. This is especially true in larger organizations with many employees or many facility locations. The locking policy should do the following:

- require that a systematic approach be taken to the use of locks for security purposes;
- assign specific responsibility for the development of the lock program. Where there is a formal security organization, the logical assignment is to Security. Where there is no full time professional security specialist or staff, the assignment can be given to any responsible manager; and
- make all persons who will use or have access to keys, locks or access devices, or combination information, responsible for compliance with the program requirements. This responsibility can be enforced through the regular line organization so that each employee may be evaluated on performance under this policy, along with performance in general, at salary review time.

8.4 SYSTEM INTEGRATION AND INSTALLATION ISSUES

Several issues must be considered when installing the entry control components of a protection system. At the highest level, it must be determined if the entry control functionality and the AC&D functionality are to be implemented on the same host computer or separately—that is, in fully integrated or parallel systems. Many questions must be considered, such as these:

- Will the entries and exits from a security area be under CCTV surveillance?
- Are there any requirements for local masking of sensors?
- Will there be any electronic connection between the AC&D/entry control subsystems and the contraband detection equipment?

These issues and many others must be addressed at the design stage of the protection system.

Many AC&D systems incorporate entry control features. Fully integrated AC&D and entry control systems are attractive for a variety of reasons. Often there is a reduced cost for both hardware and software to the user when a fully integrated system is installed rather than two separate systems. For example, the field panels that collect alarms also have card-reader interfaces and door-strike relays on the same board. Installation is simplified due to this integration. It is important that the AC&D system be informed when the entry control system authorizes a person to open a door, because the door sensor alarm signal must be suppressed for some period to allow the person to proceed into the area without causing an alarm. Door sensor masking happens automatically in a fully integrated system, but this function must be implemented by some other means, usually with user-provided hardware, when installing independent systems.

On the other hand, fully integrated systems may suffer performance degradation due to the integration. The reporting of alarms must take priority over handling entry control requests. Although this requirement seems obvious, laboratory testing reveals that in some systems alarms take several seconds to be received by the AC&D system because the system is busy processing entry control requests. Care must be taken when selecting a fully integrated system to ensure that system AC&D performance is not degraded by the entry control function. This is why system testing under normal, abnormal, and malevolent conditions should be performed to verify system performance. It is not sufficient to test a system under only normal operations; this level of performance may not represent the most critical operating state of the system. This limitation is partially compensated for through the use of high-speed microprocessors and communication protocols.

Entries and exits through doors, turnstiles, and gates are not normally recorded by the CCTV system. However, when the security level is sufficiently high and the traffic level is low, CCTV and time-lapse video recording may be used. Recordings of the visual information, along with entry and exit logs, can be useful in determining the sequence of events when security incidents occur. In addition to event-logging cameras, door and gate sensor alarms should be subject to the same video assessment requirements as other sensors in the area being protected.

Often the use of contraband detection equipment at an entrance is in the local alarm mode of operation. Because of the high number of nuisance alarms expected from metal detectors due to pocket clutter, metal detectors are seldom operated unattended. Security personnel are needed at the metal detector to see that procedures are followed, pocket clutter is searched, and alarms are resolved. Frequently the resolution of metal detector alarms involves manual search by patdown or by the use of a handheld metal detector. X-ray machines employed in package search require an operator to interpret the image generated. Automated image analysis of X-ray images for contraband is still years away. Although security personnel are usually in attendance at contraband screening points, it is sometimes advantageous to monitor this equipment at the central alarm monitoring station. Metal detector alarms may be monitored and the image generated by X-ray machines duplicated at the alarm monitoring station for secondary screening by security operators.

Another serious concern when designing an entry control system is the impact of fire codes. It is often desirable to maintain secure control for exit as well as entrance to an area; this is frequently difficult to implement without violating fire codes. A fire door normally must have a single-hand/single-motion exit device. Exit control hardware such as card readers and electric strikes can be installed but can be easily bypassed by any fire-rated exit hardware. Signs indicating that the fire-exit hardware is not used except for emergencies, but without stating consequences for violators, may encourage some users to bypass the exit controls. When fire doors do have controlled entrance and free exit, an additional means of local masking of the door alarm must be implemented. Masking the alarm for exits is usually accomplished through the use of a request-for-exit sensor. These infrared sensors detect persons approaching the door from inside the security area and alert the system that the door is about to be opened. This method is useful during normal operating hours at a facility. An additional method of addressing fire code requirements while maintaining secure control includes the use of delayed exit hardware, in which the door can be opened only after a short period. This allows for the use of CCTV to monitor activity at the exit or for the extension of the time delay while verifying the emergency condition. These systems have been useful at schools and other locations where false fire alarms have been initiated to disrupt normal activities. The method used is determined after careful examination of federal and local fire codes and security system implications. In no case should lives be placed in jeopardy;

however, in some facilities critical assets must remain protected even in emergencies. Examples include semiconductor fabrication plants, commercial nuclear reactors, and certain drug manufacturing facilities. In those cases, exit from the facility may lead to an additional secure but safe area or include the use of procedures.

Interfacing of biometric devices with the site's entry control system is another problem that arises during system design. Most biometric identifiers are implemented as the entire entry control system, rather than a component of a larger entry control system. Consequently, even when the biometric device has a data interface to a larger system, there is no industry standard for that interface. This sometimes forces the designer to trick components into operating in unison when combining card readers and PIN pads with biometric devices. A simple approach is to place the biometric device and the entry control system's unlock relays in series. A more elaborate integration is possible if the biometric devices have a card-read buffer or a shared data storage area. In this case, the biometric device captures the card-reader data stream. After the biometric verification is successfully completed, the device sends the buffered data to the entry control system. In this method the entry control system is not aware that the biometric device is connected. In a few cases the entry control system has a device-specific interface that allows biometric templates to be stored on the entry control system's host computer. This is an example of integration at the highest level.

8.4.1 PROCEDURES

As with any protection technology elements, entry control systems require a procedural component as well. These procedures address issues such as presenting badges upon entry, wearing them in plain view while inside the facility, and protecting the badge or other credentials when off-site. In addition, there should be a rule prohibiting the disclosure of any PIN numbers. The practice of tailgating, or allowing others behind to enter without completing the entry control process, should also be prohibited. Enforcement of this procedure is recommended. All employees should receive training on the proper use of company entry credentials and understand that this is a serious issue at the site. Encouraging employees to challenge those who try to tailgate or providing telephones near entry points to report this practice should be considered. Although it is courteous to hold doors open for fellow employees or others, this custom can compromise security at a facility, particularly if an employee has been recently terminated or if a visitor has not received authorization to enter. Along with this, employees should not allow access to other employees who have forgotten or lost their badges.

Other considerations when installing entry control equipment include determining how many tries will be allowed before an access request is invalid, what to do if access is denied this way, and establishing a preventive maintenance schedule for equipment. Regular

calibration of metal detectors should be performed. When using metal detectors, it is recommended that the procedure for those detected with metal be to remove the metal and reenter the detector. A variation of this procedure is to use handheld portable wands to scan those who have been detected. Once an object is found, it should be removed and the scan repeated. This process should be repeated until there are no further detections. It is important to repeat the scan after a metal object is found, because the detection of one piece of metal does not indicate that it is the only piece of metal. Allowing entry after finding a metal object without an additional scan can create a vulnerability in the protection system. If explosives detectors are used at a site, careful thought will be required to determine what to do if a detection occurs. This response can be problematic, because there are a number of elements that may generate a nuisance alarm, or an adversary may have been legitimately detected. If cameras are used to verify identity before access, users should be instructed or trained to remove sunglasses, hats, or other image blocking items, and told where to stand and which direction to face. In addition, random searches of packages, briefcases, and purses can be implemented along with technology components. If appropriate, a company policy on prohibited items such as guns, other weapons, explosives, drugs, alcohol, recording devices, and cell phones should be included in employee training and as a part of visitor control.

8.4.2 **ADMINISTRATION**

In addition to the procedures that complement use of entry control technology, a system of access controls will also need to be established. This system defines who gets access to the facility, during which hours, how many different levels of access are required, and where people can enter. It will also include procedures for visitor control, employees who forget or lose credentials, and other functions, such as parking passes. An explicit part of these procedures should describe access for people with disabilities or temporary medical conditions, like a broken leg or hand. Backup procedures will also be required where biometric devices are used—both for employees who are temporally unable to use the system and for visitors who cannot be enrolled. These exceptions may be handled through the use of oversized bypass gates or by directing people to staffed locations for assistance.

Procedures must exist for handling visitors. Clearly, all but the smallest or simplest facilities need a procedure to provide for the authorized access of visitors. The appropriate employee should make the request for access, and this request should include certain pertinent data, such as day and time of visit, the point of contact, and the purpose of the visit. Procedures may also require the signature of a manager to authorize the request. If biometric devices are used to allow entry, visitors need either to be temporarily enrolled in the database or the escorting employee will be required to provide access at the time of entry. The placement of

internal telephones at entry points may also be useful when handling visitors. A list of employee phone numbers or a help desk should also be provided.

Many large facilities designate a special office or manager to administer the access control process. An important aspect of these controls is database management. The access control system database should be continually updated to reflect employee separations, leaves of absence, or suspensions. In addition, it should track visitor credentials and assign a duration for their use. Access to the database should be limited and may require the consent of two employees to protect against insider tampering.

The office or individual assigned to manage access controls should also be the location that issues employee and visitor credentials. This function includes the previously described tasks, as well as replacement of old or lost employee credentials, removal of old or inactive credentials from the database, addition of new credentials, and collection of visitor credentials at the end of the visit. Because this can be a time-consuming process, it is recommended that the access control computer be separate from the AC&D host computer, particularly if this computer will also generate the credential. Personal computers are fairly inexpensive and the money saved by performing both of these functions on the same computer does not justify compromising operational security.

8.5 SUMMARY

This chapter described entry control systems and equipment for personnel entry control, contraband detection, and detection. These systems meet the objective of allowing the movement of authorized personnel and material through normal access routes while detecting and delaying unauthorized movement of personnel and material into and out of protected areas.

Methods of personnel entry authorization include credentials, personal identification numbers, and automated personal identity verification. Two types of errors are encountered in these systems: false rejection and false acceptance. Most credentials can be counterfeited. Also, during the process of entry authorization, the credential rather than the person is verified. Although personnel identity verification systems verify a unique personal physical characteristic, such as hand geometry or iris pattern, they require more sophisticated equipment and personnel to operate and maintain the system. These systems also require backup methods for access for those who cannot enroll or are temporarily unable to use the biometric device.

Contraband includes items such as unauthorized weapons, explosives, drugs, and tools. Methods of contraband detection include metal detectors, package searches, and explosives detectors. Metal detectors should be placed at entrances and exits, and explosives detectors should be placed at entrances. Explosives detection includes both bulk and trace techniques. Recently, there has been considerable activity in the area of weapons of mass destruction, including large explosives and chemical and biological agents. If these are capabilities of the defined threat for a facility, some technologies exist that can aid in detection, although considerable research is still needed to improve their performance.

An effective entry control system permits only authorized persons to enter and exit, detects and prevents the entry of contraband material, detects and prevents the unauthorized removal of critical or high value materials, and provides information to the protective force to facilitate assessment and response. The entry control system is an important part of the detection function of an integrated PPS. When combined with entry control procedures and a process for access control, entry control provides another method of delivering balanced protection-in-depth at a facility.

REFERENCES

- Bouchier, F., Ahrens, J. S., & Wells, G. (1996). *Laboratory evaluation of the IriScan prototype biometric identifier*. SAND96-1033. Albuquerque, NM: Sandia National Laboratories.
- Holmes, J. P., Wright, L. J., & Maxwell, R. L. (1991.) *A performance evaluation of biometric identification devices*. SAND91-0276. Albuquerque, NM: Sandia National Laboratories.
- Jain, A., Bolle, R., & Pankati, S., eds. (1991). *Biometrics: Personal identification in networked society*. Boston: Kluwer Academic Publishers.
- National Academy of Sciences. (2004). *Existing and potential standoff explosives detection techniques*. Washington, DC: National Academies Press.
- Rejman-Greene, M. (1998). Security considerations in the use of biometric devices. *Information Security Technical Report*. Vol. 3, No. 1.
- Ruehle, M., & Ahrens, J. S. (1997). *Hand geometry field application data analysis*. SAND97-0614. Albuquerque, NM: Sandia National Laboratories.
- Theisen, L., Hannum, D. W., Murray, D. W., & Parmeter, J. E. (2004). *Survey of commercially available explosives detection technologies and equipment*. Washington, DC: National Institute of Justice Office of Science and Technology. Available: <http://www.ncjrs.gov/pdffiles1/nij/grants/208861.pdf> [2012, April 18].
- Wright, L. J. (1987). *Proximity credentials—A survey*. SAND87-0080. Albuquerque, NM: Sandia National Laboratories.
- Wright, L. J. (1988). *Coded credentials—A primer*. SAND88-0180. Albuquerque, NM: Sandia National Laboratories.
- Yinon, J. (1999). *Forensic and environmental detection of explosives*. Chichester, England: John Wiley & Sons.

Note: SAND documents may be obtained at <http://www.osti.gov/bridge/advancedsearch.jsp>.



PPS FUNCTION **DELAY**

The second primary function of a PPS is delay. This function is addressed in Chapter 9, Delay Barriers.

CHAPTER 9

DELAY BARRIERS

To be effective, a physical protection system (PPS) must first be able to detect malevolent acts so a response force (such as security officers or law enforcement officers) can intervene. Because the response force cannot typically be posted at every single asset location, the PPS must also delay the adversary. That delay provides time for the response force to arrive or additional remotely controlled delay and response systems to be activated. For threats that originate outside the site, detection at the site's perimeter, rather than inside a building or vault, gives the security force more time to respond. Response time can be shortened by minimizing the time needed to assess the situation.

Barriers can deter or defeat certain threats. However, because barriers' effectiveness is uncertain, they are only potential obstacles. The delay they provide depends greatly on the adversary's tools and techniques. Determining realistic delay times may require testing, especially for unique barriers.

9.1 **BARRIER TYPES AND PRINCIPLES**

Access delay barriers may take the form of passive barriers, security officers, or dispensable barriers. Passive barriers include structural elements like doors, walls, floors, locks, vents, ducts, and fences. Security officers can delay adversaries who are trying to sneak in but may not be able to stop adversaries who use force, unless the officers are in fixed, protected positions. Dispensable barriers, such as chemical fogs and smokes, foams, and irritants, are deployed only when necessary during an attack. Each type of barrier has advantages, and a well-designed PPS may combine all three types.

Security officers can provide flexible, continuous delay. They can be moved around a site, and their shifts can be arranged to provide the needed coverage. However, a security officer force is expensive and can be overwhelmed by superior adversary numbers. Moreover, security officers, being human, could be compromised. By contrast, passive barriers are always in place and are fail secure, meaning that even if they fail they will provide a delay value. Many passive barriers are commercially available and thus relatively affordable and available. However, most passive barriers do not defend well against explosive attacks, and they generally affect a facility's operations and appearance. Dispensable barriers are compact and rapidly deployable. They can delay an adversary and tend to work no matter what the adversary's tactics are. However, dispensable barriers raise some safety and operational concerns, such as unwanted activation or possible injury to those exposed.

Traditional barriers (such as fences, locked doors, window grilles, masonry walls, and even vaults) are not likely to delay well-equipped, dedicated adversaries for long. To make sure the necessary barriers are in effect at all appropriate times requires special attention. Certain operations at the site, such as fire drills, movement of critical assets, or maintenance by contractors, may increase risks or decrease barrier delay, necessitating the use of compensatory measures, such as extra security officers. An additional challenge is that barriers must not unduly impede the facility's normal operations.

The selection and placement of barriers depends on the adversary's objective. An adversary who penetrates or destroys barriers on the way in toward the objective may not be delayed by those barriers on the way out. Emergency exits provide some delay from the outside but allow rapid exit from the inside. While nature provides some barriers in the form of rugged coastlines, high cliffs, and vast distances, in most cases barriers must be carefully and deliberately placed in the adversary's path. The delay that barriers provide depends on the particular obstacles employed and the tools used to breach them.

An example of deliberate placement would be to install detection systems and barriers next to each other so adversary encounters first the sensor and then the barrier. Such an arrangement delays the adversary at the point of detection, increasing the probability of accurate assessment.

According to the principle of balanced design, each aspect of a barrier configuration should provide equal delay—that is, there should be no weak links. An adversary will not burn a hole in a door to crawl through if the door's hinges are clearly easier to defeat. Delay-in-depth is analogous to protection-in-depth for detection systems. Placing several layers of varying barrier types along all possible paths the adversary could take complicates the adversary's task. Upgrading a barrier to force the adversary to use more sophisticated tools raise's the adversary's logistics, training, and skill requirements even if it does not always increase the penetration time.

Generally, the security barriers at industrial facilities are designed to deter or defeat infrequent acts of casual thievery and vandalism. In an environment of escalating threats, traditional fences, walls, doors, and locks may not present enough deterrence or delay. The more the adversary is delayed, the more time security staff have to assess the situation and send a response force. A few minutes of delay can make a significant difference in the intrusion's outcome.

A barrier is considered penetrated when a person passes through, over, under, or around it. This chapter assumes that the penetration effort begins 2 ft. (.6 m) in front of the barrier and ends 2 ft. (.6 m) beyond it. Penetration time includes the time to travel through the barrier. For example, cuts through concrete and rebar in may be very jagged, and cuts made with thermal tools may require cooling, adding to the barrier's delay time. Likewise, very thick walls require a larger-diameter crawling hole than do thin walls, increasing the barrier's delay time.

A vehicle barrier is considered penetrated when (1) a ramming vehicle passes through or over it and is still a functioning vehicle or a second vehicle is driven through the breached barrier or (2) the vehicle barrier is removed or bridged and a functional vehicle passes through or over it. The choice of barrier depends largely on the type of vehicle that may be used in an attack. A chain-link fence might be able to stop a motorcycle or a small all-terrain vehicle but would be ineffective against a large truck.

As the adversary meets increasingly difficult barriers, it becomes harder to transport and set up sophisticated tools, especially if the adversary must crawl through several small openings. The distance from vehicle areas to the target area also makes a difference. If the adversary has to carry heavy equipment a long way, delay increases significantly. Some facilities set up barriers outside perimeter detection to force adversaries to change tactics and abandon their vehicle. Forcing them to walk or run and to carry their tools slows them down, but until they are detected this extra delay is not included in system effectiveness measures. Vehicle barriers outside the detection and assessment zone are not recommended.

Barrier penetration time depends in part on the method of attack, including the necessary equipment. Attack tools considered in this chapter are as follows:

- hand tools—sledgehammers, axes, bolt-cutters, wrecking bars, metal cutters
- powered hand tools—hydraulic bolt-cutters, abrasive saws, electric drills, rotohammers, abrasive water jets
- thermal cutting tools—oxyacetylene torches, oxygen lances
- explosives
- vehicles—trucks, automobiles, trains, boats, planes, helicopters, motorcycles, and ATVs

Battery-powered tools have improved greatly over the past decade. They can now power small hydraulic systems and all types of cutters, and they are light, powerful, and disposable. They should be considered when evaluating delay elements of a physical protection system. Because of these new capabilities, enhanced or new barriers may be needed to increase delays enough for an appropriate response.

9.2 PERIMETER BARRIERS

Perimeter barriers, the outmost protective layer of a physical protection system, are intended to exclude unauthorized personnel from an area. Ordinary chain-link fences constitute a visible legal boundary around a facility and provide a means of posting signs regarding trespassing, security measures, or even use of deadly force. However, such fences do not pose a serious obstacle to a dedicated adversary. In seconds, a person can ram through the fence with a vehicle, climb over it, crawl under it, or cut through it. Barbed tape and concertina wire add only a little delay value. In a minute or less, a person can use portable bridging aids (e.g., ladders and ropes) to cross over almost any type of perimeter barrier that is a few yards high and on the order of 30 ft. wide.

Still, upgraded perimeter barriers provide several significant benefits:

- Coupling vehicle and personnel barriers into a perimeter, inside and adjacent to the perimeter detection system, delays the intruder at the point of detection, improving the assessment function.
- Delaying the intruder at the perimeter may enable the response force to intercept the intruder near the point of the alarm. Without a delay, the intruder will likely have left the alarm point by the time the response force arrives.
- They make it possible to protect a site whose targets are assets stored in several easily penetrated buildings on-site.
- Vehicle barriers around a site's perimeter (inside the perimeter sensors) may force an intruder to travel on foot and to carry any needed tools and weapons.

9.2.1 **FENCES**

One cannot prevent intrusion solely by topping fences with rows of barbed wire, general-purpose barbed-tape obstacle, or barbed-tape concertina (BTC). However, rolls of barbed tape on or near standard fences can increase fences' delay capability (Kodlick, 1978).

One of the most cost-effective additions to a fence is to attach a roll of barbed tape to the outriggers, as the tape forces an intruder to bring additional aids or bulky equipment to climb over the fence. The direction of the outriggers makes little difference in fence climbing times (Kodlick, 1978), though directing the outriggers to point toward the inside does eliminate the handgrip used by intruders when climbing over the fence.

In addition, barbed-tape rolls can be placed horizontally on the ground or against the fence material. Typically, barbed-tape rolls are placed inside an outer perimeter fence and outside an inner (double) fence. This arrangement prevents accidental injury to casual passersby, both outside and inside the site. Rolls placed horizontally should be staked to the ground, and maintenance will be required, such as preventing excessive plant growth and debris from clogging the rolls. Rolls of barbed tape tend to obscure CCTV views in the clear zone, thereby increasing assessment time.

It typically takes several minutes to penetrate a fence that is fortified with barbed-tape rolls. The few minutes of delay that BTC mounds add may not be worth the cost, especially for larger sites (Kane & Kodlick, 1983).

9.2.2 **GATES**

Gates establish points of entrance and exit to an area defined by fences and walls. They limit or prohibit the flow of pedestrian or vehicular traffic and establish a controlled traffic pattern. Gate barriers and perimeter fences at a site should provide equal levels of delay. Gate hinges, locks, and latches may require additional hardening.

Because gates often directly face driveways, gates may be especially susceptible to ramming by a vehicle. Carefully choosing the orientation of vehicle gates and their driveways may reduce the probability of a vehicular breach. Laying out driveways with multiple turns on each side of the gate reduces the approach and departure speed that vehicles can attain.

One way to upgrade vehicle portals is to use several hardened gates at the perimeter. The gates can be interlocked, requiring one gate to be closed and locked before the other can be opened. The space between the gates provides a holding area and provides more time for determining whether contraband materials or unauthorized persons are attempting to enter or leave.

9.2.3 **VEHICLE BARRIERS**

Private motor vehicles should be kept out of secured areas as much as possible, as they can be used to introduce tools and explosives, even without the driver's knowledge. Cars and trucks can crash through most fences. Vehicle barriers should be installed inside the detection and assessment zone to ensure valid delay. The following are key steps to take when selecting the type and location of the vehicle barrier system:

- Define the threat the barrier system is intended to stop, considering weight, impact speed, and other physical characteristics.
- Define the asset and determine the area to be protected.
- Examine the site, studying terrain, road layout in and around the secured area, buildings and parking lot locations, climate, and traffic patterns around the area.
- Keep the entire physical protection system in mind.

Once a barrier system has been laid out, the next step is to select types of barriers that are best suited to protect against the defined threat vehicle. Proper installation is essential. In areas that cannot be monitored continuously but may be periodically checked by roving security officers, it makes sense to install barriers that are hard to defeat. Concrete-filled pipes can be installed to delay an adversary long enough to be detected by a security officer. By contrast, cable barriers can be defeated easily with hand-carried cutting tools. Cable barriers should be used only in areas that are well patrolled or else sensed and under CCTV assessment. Optimum barrier height depends on the type of vehicle but is typically about 30 in. (76 cm) (Sena, 1984).

All barriers can be breached if the adversary is allowed enough equipment and time. Denying rapid vehicular access forces the adversary to carry any tools or breaching aid to other barriers or to spend trying to move the vehicle through the vehicle barrier. Keeping the adversary from using a vehicle to penetrate the area slows him or her down inside the area and also slows escape.

A barrier system must be able to stop a defined threat vehicle at a specific distance from a secured area, regardless of where the attack begins. The stopping capabilities of stationary and movable barriers must balance each other to avoid any weak links in the system. In some cases, two-way protection with barriers may be needed.

For the vehicle to be stopped, its kinetic energy (proportional to the square of its velocity and to its mass) must be dissipated. Most vehicle barriers are designed to stop vehicles through one or more of these methods:

- **Vehicle arrestor.** This absorbs most of a vehicle's kinetic energy, applying a low to moderate resistive force to stop a vehicle gradually over a relatively long distance. Examples are weights that are dragged by a vehicle and accumulate with distance traveled, or piles of loose sand.
- **Crash cushion.** This absorbs much of the vehicle's kinetic energy, providing a stiff resistive force to stop a vehicle in a shorter distance. Examples include liquid-filled plastic containers and arrays of empty steel barrels backed by strong supports.
- **Inertia device.** This exchanges momentum and kinetic energy with a vehicle during impact, using a stiff resistive force to stop a vehicle in a shorter distance. Examples include relatively small concrete shapes and unanchored, sand-filled barrels.
- **Rigid device.** This provides very highly resistive force to stop vehicles in very short distances. The vehicle dissipates almost all of its own kinetic energy as it deforms during impact. Examples include massive concrete shapes and well-anchored steel structures.

The U.S. Department of State formerly set performance standards for both perimeter and portal vehicle barriers. A new standard is ASTM F 2656-07, which applies to fixed vehicle barriers. It specifies how tests should be conducted; what a test range must do to be certified; what vehicle types, weights, and speeds to use; and what the penetration ratings are. The 16-page specification can be purchased from ASTM. The ratings range from small cars at moderate speed to heavy dump trucks at high speed. Rated vehicle barriers range in thickness from less than 1 meter (3.3 ft.) to more than 30 meters (98 ft.).

9.3 STRUCTURAL BARRIERS

Structural barriers include walls, doors, windows, utility ports, roofs, and floors. Most industrial building walls and locked doors can be penetrated in less than a minute, and windows and utility ducts provide intruders with additional routes for entry or exit. Expanded metal grilles offer little delay to determined adversaries. In less than five minutes, an adversary with explosives and cutting tools can make a crawl hole through a reinforced, 18-inch thick concrete wall. Tests at Sandia National Laboratories show that the concrete is readily removed by the explosive charge (White, 1980).

Hardening a normally constructed building against forcible penetration for a significant period is rarely practical or cost-effective. In addition, because doors must be open or unlocked during working hours for operational needs and for use as emergency exits, doors provide an easy adversary path through walls. The delay that can be achieved through building hardening is limited.

9.3.1 **WALLS**

Walls are generally more resistant to penetration than are doors, windows, vents, and other openings. Still, most walls can be breached with the right tools. In fact, a wall may be an adversary's best path for forcible entry. Large vehicles can ram through cinder block, wood frame, and many other common wall types. Depending on the strength of the wall and the type of vehicle, the vehicle may or may not be operable after the impact.

Explosives can produce holes large enough to crawl through. Upgrading walls or increasing their thickness usually adds only a moderate delay against explosives, even though the amount of explosive needed increases substantially with wall thickness. Upgrades may be more effective in extending the penetration delay against hand, power, or thermal tools.

These are the most common types of walls in facilities:

- reinforced concrete
- expanded metal/concrete
- concrete block
- clay tile
- precast concrete tee sections
- corrugated asbestos
- sheet metal
- wood frame

Reinforced concrete walls are commonly used in structures where sensitive materials are used or stored, and they are widely believed to be formidable barriers. However, testing has shown that ordinary reinforced concrete walls can be penetrated quickly (White, 1980). They are generally designed to support structural loads, not to thwart or delay penetration. In conventional construction, structural requirements, not security needs, typically determine the strength and thickness of concrete and the size and spacing of reinforcing materials.

Placing two or more reinforced concrete walls in series results in longer penetration delays than using one wall that is as thick as the two walls combined. To penetrate multiple walls requires multiple individual efforts and transporting of tools through preceding walls. If explosives are used, contained pressure from the explosion could collapse the roof and surrounding structures, creating further barriers in the form of rubble.

Reinforcement of concrete generally extends penetration delays. Even after an explosion, rebar usually remains intact, at least enough that the adversary must remove it before passing through. Removing the rebar often takes longer than removing the concrete. Delay

can be increased by using additional rebar, increasing rebar size, or decreasing center-to-center rebar spacing.

Another way to increase delay is to use earth cover or other overburden to delay access to the wall itself. Overburden is a cheap yet effective defense against all methods of attack.

9.3.2 **DOORS**

The weakest portion of a barrier determines the barrier's ultimate value. The principle of balanced design applies particularly to doors. Doors are classified as follows:

- standard industrial doors
- personnel doors
- attack- and bullet-resistant doors
- vehicle access doors
- vault doors
- blast-resistant doors
- turnstile gates

The penetration delay provided by walls can be increased with thicker or composite materials. Doors, however, tend to be a weak link in a structure because of their functional requirements and associated hardware. For example, many buildings with heavy concrete walls offer pedestrian access through hollow steel doors. The barrier value of the walls is relatively high, but it is weakened by the use of ordinary doors, frames, and hinges.

The principle of balanced design requires that doors and their associated frames, hinges, bolts, and locks be strengthened to provide the same delay as that provided by the floors, walls, and ceilings of the parent structure. If the door assembly cannot be sufficiently enhanced, it may not be cost-effective to upgrade the building structure. In recent years a number of major door manufacturers have made attack- and bullet-resistant door. When properly installed, these doors increase penetration resistance.

Most common exterior doors are 1¾ in. (44 mm) thick with 16 or 18 gauge (1.5 or 1.2 mm) steel surface sheets. Construction is usually hollow core or composite, and the door may feature glass or louvers. A composite door core contains noncombustible, sound-deadening material, usually polyurethane foam or slab. Light-gauge vertical reinforcement channels are sometimes used inside hollow core doors to add strength and rigidity.

Steel pedestrian doors are found in single or double configurations. Exterior doors usually swing outward and have their closing devices attached internally. Hinges are mortised with

either removable or nonremovable pins. Panic bars on emergency exits make those doors only a one-way barrier. Such doors are easier to defeat on the way in, and they also make it easier for an attacker to leave the building. In some cases, a 30- to 45-second delay system can be incorporated at the emergency exit door. Under normal circumstances, the delay mechanism prevents opening of the door for the prescribed time. However, if a fire alarm is pulled or the automatic fire suppression system is activated, the delay mechanism is overridden.

Penetration times for standard, lightweight sheet steel doors vary. An attack with explosives is loud and produces obvious evidence of penetration, which can help in detection of an attack. Attackers may also use thermal cutting tools. Power tools can produce a hole big enough to crawl through in three minutes.

Standard key locks, if accessible, are susceptible to being picked. The picking time depends on the type and condition of the lock but averages about one minute for a skilled locksmith. By using a pipe or strap wrench on a key-in-knob lock, an intruder can enter in well under a minute. Picking tools work only if a keyway is available, and a pipe wrench works only on exposed locking hardware. Doors that need no entrance mode (strictly exit) can be fully flush-mounted with no external hardware. If keyways are required, greater delays may be gained from high-security locks with long pick times. The use of door sensors reduces lock vulnerabilities.

On external doors, hinge pins are usually exposed and thus are natural targets of attack. Even nonremovable hinge pins can be defeated quickly with hand tools. Thermal tools or explosives can also be used. Only about a minute is required to defeat the (usually three) hinges on an external door. Louvers, windows, and mesh on doors can be penetrated with hand tools, which can also create a crawl-through hole in plate, tempered, or wired glass in 15 seconds. It takes only 30 seconds to force apart louvers or mesh.

External doors are susceptible to vehicle ramming. Search and rescue tools, too, may be used, such as special shotgun rounds used by police to breach doors, and hydraulic spreaders used by fire departments.

To match the delay provided by the overall structure, improved designs are needed for industrial doors. Penetration times for industrial doors vary greatly, starting at 10 seconds. Internal panic bars may be required by fire and building codes.

When complete door replacement is not an option, older standard doors can be upgraded. At new facilities or where complete door replacement is necessary, new high-security, attack-resistant doors should be installed.

Existing structures often feature steel pedestrian doors mounted in stamped steel frames. Such doors offer little resistance to forcible attack but can be upgraded to better resist attacks with hand, power, or thermal tools.

Eliminating unnecessary doors is the first step in upgrading a facility's resistance to penetration. Eliminating unneeded windows, louvers, and external knobs and keyways is the next step. Adding steel plates to door surfaces increases penetration resistance against hand and light power tools. Added weight can be supported with heavy-duty hinges, and grouting frames with concrete can strengthen the supporting structure. Placing wood cores, especially redwood, between door plates increases the delay time for thermal cutting tools by three to four times that of an air void.

Attackers can use hand tools to attack the lock/frame area of a door, forcing the frame strike away from the lock bolt. A forced separation of ½ in. (13 mm) to ¾ in. (19 mm) is usually enough to pry open a door. To prevent easy access to the lock/frame area, a sheet steel strip can be welded or bolted to the door. The strip should be the same height as the door and at least 2 in. (51 mm) wide with a 1 in. (25 mm) overlap onto the adjacent doorframe. The door frame should be grouted with concrete at least 18 inches above the frame strike location, on both sides of the frame. Exterior pedestrian doors should be fitted with high-security locks. Replacing a single conventional lock with a high-security, multiple-deadbolt system would virtually eliminate prying attacks.

Hinges can be compromised in about one minute either by removing the pins or cutting the hinge knuckles. Welding the pin top to the hinge extend penetration times if only hand tools are used; however, if the hinge knuckles are cut with power or thermal tools, the penetration time is still only about one minute. Upgraded hinges with a stud-in-hole feature can extend penetration time. Another way to prevent hinge-side door removal is to bolt or weld a steel Z-strip to the rear face of the door. If the hinges are removed and an attempt is made to pry the door from its frame, a leg of the Z-strip will come in contact with either the inner frame surface or the rear doorstop surface. Once the Z-strip contacts the doorframe, adversaries must use greater force and larger tools to remove the door. Full-length hinge designs may also extend penetration times significantly.

Panic (or crash) bars can be defeated in about 1 minute with small hand tools, which produce less noise thermal cutting. If noise is not a factor, hand or power tools can be used. One way to upgrade a panic bar-equipped door is to install a bent metal plate with a drill-resistant steel section fastened to it. The plate prevents chiseling and wire hooking of the panic bar. The drill-resistant section extends penetration time considerably if the area between the panic bar and the horizontal leg of the plate is attacked. Emergency exits may also use electronic control devices that require the push bar to be depressed for a set period before an electronic deadbolt is released. This delay allows a security officer time to assess

the situation via CCTV and to respond if necessary. Another recommendation is to remove exterior doorknobs and other hardware from emergency exit doors. Doing so hinders prying attacks from the outside but does not compromise rapid emergency egress.

Because louvers and glazing material can be penetrated easily with hand tools, their use should be minimized for exterior doors. If still needed, they should be reduced in size so no one can crawl through. They can also be strengthened with a screen or bar grid inside aperture.

9.3.3 **WINDOWS AND UTILITY PORTS**

Without enhancement, windows delay adversaries only slightly. Windows should follow the balanced design principle so they will not be the weak link in a barrier system. This section describes frames, glazing materials, protective coverings, and other means of improving window penetration delay times.

Aside from doors and windows, industrial facilities have many unattended structural openings, such as ventilating ducts, utility tunnels, and service openings, which can be used as intrusion paths. Especially if openings are designed to provide easy access for maintenance, few structural openings would delay a determined adversary for long. Because such openings offer concealed pathways, they should be barricaded and sensed. *Utility ports* are all types of unattended framed openings aside from doors and windows. Any grilles they feature may provide safety or ornamentation, or they may keep out pests, but they provide little security. Standard windows and utility ports constitute potential weak links in a barrier system. Most unenhanced windows can be penetrated with hand tools in less than 30 seconds. Utility ports may feature covers that are not locked or protected with interior barriers.

Window frame strength and weight vary widely. Some manufacturers offer a security sash but fail to harden the frame material. When windows are installed in doors, they can usually be penetrated in a few seconds with hand tools. Some special window frames contain concealed materials that resist cutting. In a window that can be opened and closed, the window-locking mechanism may be a weak link, allowing the window to be opened if the mechanism is forced. The locking mechanism should not be readily accessible from the exterior. Upgrade options include fixed windows or more substantial locking devices.

The attachment of the window frame to the structure can be strengthened with additional or heavier fasteners or by welding the frame in. Delay time through the window may not be increased unless additional upgrades are made to the glazing materials and protective coverings. Glazing materials include standard, tempered, wire, and laminated glass. These barriers defend against the elements but not against intruders.

Standard glass is highly frangible. Penetration with hand tools generally takes only a few seconds. For greater penetration resistance, thick security glass can be used. In addition, standard glazing materials are often upgraded with a protective grill of expanded steel mesh or other forms of metal grills. Tempered glass, formed through reheating and sudden cooling, features greater mechanical strength and better thermal stress characteristics, but it can be broken with handheld impact tools in a few seconds.

Wire glass is used often in fire doors and fire windows. The ¼ in. (6 mm) thick material is fabricated with diamond, square, or hexagonal wire patterns. Wire glass can be penetrated with hand tools in about 20 seconds. Laminated glass is made of two or more panes of annealed float, sheet, or plate glass bonded to a layer or layers of plastic. Safety glass that is ¼ in. (6 mm) thick can be penetrated in 30 seconds, while 9/16 in. (14 mm) security glass requires 15 minutes of work with hand tools to produce a crawl-through hole. Security glass is not transparent armor, but it resists forcible penetration better than standard glass.

Sometimes transparent plastics can substitute for glass, though some types are combustible and their use may be restricted by fire codes. Acrylic plastics like Lucite™ and Plexiglas™, if less than 1 in. (25 mm) thick, can be broken with hand tools in less than 10 seconds. Polycarbonates, by contrast, resist impact about as well as bullet-resistant glass. Tests show that ½ in. (13 mm) thick Lexan® resists hand-tool penetration for up to two minutes (Nuclear Security Systems Directorate, 1989). Thermal tool attacks require about one minute but also cause combustion and the release of toxic gases.

Glass/polycarbonate composite glazing contains a tough core of polycarbonate between two layers of glass. The glazing was developed for use in prisons. In tests, glass/polycarbonate composites were penetrated when hand tools and fireaxes were used, but the thickest panels lasted 10 minutes against miscellaneous steel tools (Nuclear Security Systems Directorate, 1989).

The penetration resistance of windows and utility ports may be increased with grilles, bars, expanded-metal mesh, or screens. Grids and grates made of steel mesh, expanded metal, bar stock, tubing, or bars can be used to reduce the size of the opening in utility ports to keep someone from crawling through. These coverings should be placed at or after appropriate detection measures. Window improvement should be guided by the balanced design concept. With proper enhancements (protective coverings, grills, mesh), different glazing material, or upgraded methods of frame attachment, the delay time of windows may approach the delay time of doors or even walls for some threats.

Most tunnels used to link buildings are not protected very well. Access may be controlled only by unlocked lift-off covers or manholes. Pipe channels inside buildings are often congested but still allow space for maintenance work. Ducts associated with heating, ventilating, and air

conditioning systems could provide an adversary path. Tunnels, manholes, roof and wall openings for equipment, and ductwork can be enhanced with interior barriers.

For new buildings, designers should consider smaller-than-man-size windows and multiple, small openings for utility ducts. The use of very narrow windows—4 in. (102 mm) or less—increases penetration time, since even with the glazing removed, the opening will need to be enlarged to create a person-size hole. Some windows could be removed from existing structures to allow the original window opening to be upgraded to the same penetration delay as the adjoining wall.

9.3.4 **ROOFS AND FLOORS**

Roofs and floors keep out the weather, provide spaces on which to work, and serve as protective barriers. In considering their security value, one should examine penetration threats from determined adversaries using a combination of hand, power, and thermal tools, as well as explosives.

Roofs and floors are constructed using similar methods, but they vary in thickness, type and quantity of steel reinforcement, and concrete strength required to carry the loads. In general, compared to roofs, floors offer more resistance to penetration because they are protected by the main structure and are designed to accommodate heavier loads.

Contemporary roof types include the following:

- prestressed concrete tee beam
- metal subdeck and reinforced concrete
- metal roof deck with lightweight concrete
- metal roof deck with insulation
- metal roof
- reinforced concrete beam and slab
- wood sheathing with membrane

Roofs, both new and existing, can be enhanced in several ways. Improvements below the roofline generally provide the best value. The following are among the methods of roof enhancement:

- enhancing membranes with embedded screen
- adding several inches of rigid insulation
- using concrete reinforced with deformed steel bars and expanded steel mesh
- forming larger rebar into several rows or layers for reinforced concrete

- increasing the number of fasteners and adding structural members to corrugated roofs
- using mechanical fasteners or joints and a continuous weld and heavier gauge material on metal roof systems
- using larger rebar to strengthen the flange area of precast concrete tee beams

Penetration tests suggest that barriers placed below the roof may be more effective against penetration than those in the roof itself. In some structures, such barriers can be added without making significant modifications. Employing enhancements below the roofline could force the adversary to make a second penetration, and that second penetration could well be in a confined space and require different types of tools, adding to the adversary's challenge. The optimum distance between the roof and the secondary barrier is 10 to 12 in. (254 mm to 305 mm). The small space can create a hole effect or cramp the adversary's efforts to penetrate the next barrier. Enhancement materials include quarry screen, expanded steel bank vault mesh, and floor gratings.

Adding an earth covering can increase the delay through both the roof and the walls. Both buried and cut-and-cover structures use an earth covering to delay access and protect against blasts.

9.3.5 **DISPENSABLE BARRIERS**

Dispensable barriers are deployed only when necessary (specifically, during an attack), and they may be active or passive.

Active dispensable barriers can—when activated—stop or delay an adversary from accomplishing the objective. A typical active dispensable barrier system includes these elements:

- a process for deciding when to activate the dispensable barrier
- command and control hardware
- material that is deployed to delay access or incapacitate the adversary
- a dispensing mechanism
- security officers on-site

The decision process may start with a security officer, an intrusion sensor, or a combination of the two. Appropriate hardware design and operational procedures can help in striking the right balance between ensuring that activation occurs in an attack and minimizing the risk of inadvertent activation.

The command and control hardware receives the activation decision and operates the dispensing hardware. Thus, command and control hardware stands between the decision

mechanism and the dispensing hardware, which may be widely separated. Thus, it is necessary to consider the risk that the process could be interrupted by electromagnetic radiation, lightning, earthquakes, power surges, and other severe conditions. The command and control hardware makes it possible for personnel in the area to avoid hazards if inadvertent activation occurs.

The dispensable material, normally stored in compact form, expands to an effective delay state through a chemical or physical reaction. Dispensing hardware is unique for each material and application but typically consists of storage tanks, activation valves, pressure regulators, safety valves, filters, power sources, and plumbing hardware. Dispensing hardware tends to be expensive, and it must be secured so an adversary cannot use or disable it.

Dispensable barriers force the adversary to defeat the barrier and evade the response force. Such barriers often isolate the adversary visually, acoustically, at a particular location, or all three. This added challenge for the adversary increases the chance that the overall physical protection system will perform as desired.

Passive dispensable barriers present many of the same benefits but do not require a command and control system. Instead, the adversary's penetration attempt activates the dispensing mechanism. Eliminating command and control hardware makes passive dispensable barriers much cheaper than active dispensable barriers.

Structural barriers have an appealing simplicity, yet dispensable barriers are sometime cheaper and may fit better with operational needs at the site. Dispensable materials and related hardware that are being developed and tested include rigid polyurethane foam, stabilized aqueous foam, smoke or fog, sticky thermoplastic foam, and various entanglement devices.

Rigid foam has been used for storing assets or protecting them in transit. Stabilized aqueous foam, which has been used at government sites abroad, is also a fire retardant, adding safety benefits. Irritants, including pepper mace, can be added to aqueous foam to further delay an adversary. Smokes and fogs are easy to dispense with commercially available dry ice or other fogging machines (like those used in theatrical applications). Sticky foam has already been used in specialized applications and has been considered for use in less-than-lethal applications, such as prison cell extractions or crowd control. Entanglement devices include coils of wire or nets suspended from ceilings and the dropping of shredded paper onto an adversary. Such items work best in combination with smoke or fog barriers, which can conceal the entanglement devices. Safety is an important consideration when deciding whether to use certain dispensable barriers.

Dispensable barriers are usually deployed very near the assets being protected. That placement is both the most effective location (as it is easier to fill a small space with smoke or fog than a large one) and the most affordable. Employing the dispensable materials close to the target (ideally in the room where the assets are stored), minimizes cleanup and collateral contamination.

The various dispensable materials all have their strengths. Choosing the best material for a given application requires balancing the following strengths of different dispensable barriers:

- minimum impact on operations
- ability to protect volumes
- safety for personnel
- ability to operate independently of barriers
- multiple activation options
- long storage life
- provide protection-in-depth
- can be cost-effective

Technologies that combine delay and response are currently being developed and deployed to protect high-value assets. For example, a new remotely fired weapons system is operated by a security officer in a remote, well-secured location. Removed from the danger, the officer can better assess the situation and respond appropriately. Another system uses millimeter waves to produce a severe burning sensation in the adversary's skin (but no physical harm), driving the intruder away.

9.3.6 **PROCEDURES**

Most passive barriers require only normal cleaning, periodic inspection, or upkeep. For example, fences, doors, and windows should be repaired or replaced if loose or broken. Maintenance procedures for dispensable delay systems vary widely. Passive dispensable systems must be checked for obvious damage and appropriate pressure in pressurized designs. Active dispensable systems require routine testing of the command and control system. Dispensable delay systems tend to last 10 to 25 years.

Some access points—utility ports, ducts, or drainage pipes—can be equipped with sensors to provide an alarm when disturbed. Placing the sensor where it will be activated early in the delay time of the access point can create an effective combination of detection and delay.

9.4 **SAFES**

Safes can make an important contribution in any security program, but because a container is called a safe, it does not necessarily follow that it will properly protect everything stored in it. The characteristics and limitations of various types of safes must be understood. A safe designed for fire protection would not be effective in preventing a forced entry. Materials used to dissipate heat may do little to resist the blow of a hammer. A safe designed to protect money will give little protection against fire because its thick, solid steel walls transfer heat rapidly to the interior. Paper will be destroyed quickly by a fire in such a container.

A labeling service has been established by Underwriters Laboratories Inc. (UL) to define the level of protection each safe can be expected to provide. The various labels and standards for classification of each are discussed later.

Safes of the type included in this discussion can generally be classed as portable. That is, unless anchored in place, they can be moved with basic and readily available equipment. Even if a container is classed as burglary resistant, it might be removed from the premises intact to be penetrated at the thieves' convenience. A safe on wheels is not burglary resistant. A container of this type, in an isolated area without some other type of protection such as alarms or surveillance, should be considered vulnerable. UL standards require that a safe weighing less than 750 lb. (34 kg) be anchored.

This section examines (1) record safes designed for fire protection and (2) safes designed for protection of valuables against forcible penetration.

9.4.1 **RECORD SAFES FOR FIRE PROTECTION**

Records are the lifeblood of every organization. Records volume has been constantly increasing, and records' format has changed to include magnetic media (such as discs and tapes), which are more vulnerable to heat and flame than is paper.

Records can be protected in safes that have been scientifically insulated and constructed to resist damage from high temperatures resulting from both heat and flames. A record safe typically incorporates moisture in its insulation to help dissipate a fire's heat so the interior temperature does not rise to the point where records are destroyed. Once lost, such moisture cannot be replaced. For that reason, a record safe that has been exposed to a fire might not be able to protect records. Moisture also evaporates overtime. A fire-resistant safe keeps its rated value for about 20 to 30 years, depending on climate.

The level of protection to expect can be determined on labels found on safes approved by UL or the former Safe Manufacturers National Association (SMNA). The labels are usually on the

back of the door, but they may also be found on the exterior of the safe. Although SMNA no longer exists, one may still encounter safes carrying their former labels.

UL used letter classifications until 1972, when its labels began to list the type of container and the level of protection. UL labels now indicate whether the container is a fire-resistant safe or an insulated records container (differences discussed below). In addition, UL labels now indicate the hours of protection and the temperature that the inside of the container can withstand. For instance, the designation “350°—4 Hours,” indicates the safe contents will endure a temperature of 350°F (177°C) for four hours. Paper could be expected to be protected for four hours in this class of container. (The same classes of fire resistance as those used in UL labels are defined in NFPA 232, Standard for the Protection of Records.) For magnetic media protection (150° safes), the relative humidity of the protective container during the rated protection period is higher than for conventional (350°) safes, the former being 80 percent and the latter 65 percent.

This section discusses three types of safes designed for record protection: fire-resistive safes, insulated filing devices, and containers to protect magnetic media.

Fire-Resistant Safes

Fire-resistant safes may be labeled as follows:

| SMNA | FORMER UL | PRESENT UL |
|------|-----------|-------------|
| A | A | 350—4 hours |
| B | B | 350—2 hours |
| C | C | 350—1 hour |

All three classes must pass tests against fire, explosion, and impact. During the fire endurance test, the inside temperature of a safe is recorded and cannot exceed 350°F (177°C). At the end of the tests all papers inside the safe must be entirely legible and not crumble or fall apart during removal and examination.

Insulated Filing Devices

Insulated filing devices, designated Class 350-1 (formerly Class D) and Class 350-1/2 (formerly Class E) afford considerably less protection for records than the three levels of fire-resistive containers. In the test procedure the thermocouples for measuring interior test heat are placed in the center of the interior compartment, whereas in first-resistant safes they are located one inch from the sides and door. Insulated filing devices are not designed to be drop tested as are the fire-resistant safes and record containers. As it is possible to confuse the

350-1 insulated filing device with the 350-1 fire-resistant safe and 350-1 insulated record container, the label should be carefully noted. A label will indicate whether a container is a fire-resistant safe or record container, or if it is an insulated filing device.

An insulated filing device may be expected to give protection only against burnout in fire-resistive buildings where the area around the container has a small quantity of combustible material. (A fire-resistive building is defined by NFPA Standard 220 as “one in which all structural members including columns, beams, floors and roof are of approved non-combustible or limited combustible materials” with specified resistance ratings.) Also, insulated filing devices should not be stored on a floor that might collapse during a fire because if they dropped they could break open, allowing the contents to be damaged or destroyed.

Electronic Data Processing Record Protection

Computers and electronic data storage media pose a new records protection problem. Because magnetic media begin to deteriorate at 150° F (66° C) (lower at humidity levels of more than 80 percent), record containers designed to protect paper cannot be used to protect magnetic and other media. What is needed is a container that can withstand high humidity levels as well as extreme heat.

One approach is the “safe within a safe,” consisting of a sealed inner insulated repository in which the magnetic media are stored, along with an outer safe protected by a heavy wall of insulation. This type of container has been designed to protect electronic records against 125° F (52° C) or 150° F (66° C) and 80 percent humidity for four-, three-, two-, or one-hour periods. Other models provide the same protection without the safe within a safe.

Labels on the containers should indicate the UL ratings against fire exposure for between one and four hours. The labels designating the containers’ protection capabilities are shown in Figure 9-1.

In the fire-endurance test, the container is loaded with recorded tapes, discs, and microfilm. Two temperature limits are employed: 150° F (66° C) for magnetic tape and microfilm, and 125° F (52° C) for diskettes.

The container is placed in a test furnace that starts with an interior temperature of 70° F (21° C). The fire is continued at the rated temperature for the period required by the test, after which it is extinguished and the equipment allowed to cool without opening the furnace. During the cooling cycle, the interior temperature and relative humidity are recorded until a temperature of 120° F (49° C) is reached. A second unit is also subjected to the fire impact test—a 30 ft. (9 m) drop after heating.

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Insulated Record Containers and Fire-Resistant Safes Class 25-4 hours Class 150-4 hours Class 125-3 hours Class 150-3 hours Class 125-2 hours Class 150-2 hours Class 125-1 hour Class 150-1 hour | Insulated Filing Devices Class 125-1 or ½ hour Class 150-1 or ½ hour Insulated File Drawer Class 125-1 hour Class 150-1 hour |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Figure 9-1
Underwriters Laboratories Label Designations

After the fire endurance test record container has cooled to normal temperatures, it is opened and examined for visible evidence of moisture penetration into the interior, and to determine the condition of the contents. The media are then used on a computer to determine their readability. The safe passes the test if the information loss after the fire does not exceed 1 percent.

9.4.2 **SAFES DESIGNED TO PROTECT VALUABLES**

Containers designed for burglary protection are classified in accordance with test data and specifications that conform to requirements of the Insurance Services Office and UL. Safes of this type generally do not protect against fire. If both valuables and fire protection are necessary, a valuables container can be installed in a larger safe or vault designed for protection against fire, or a safe rated for both fire and burglary can be used. The interiors of valuables safes are usually smaller than the interiors of record safes because money and valuables typically require less space than records and business papers. To prevent this type of safe from being removed, it should be installed in a steel-clad concrete block or be otherwise securely anchored.

Burglary-Resistive

Burglary-resistive equipment resists an attack in which the burglar uses tools, a torch, or explosives and has sufficient time to work. This type of equipment is made of laminated or solid steel. Laminated steel is defined as two or more sheets of steel, with the facing surfaces bonded together, with no other material between the sheets. It is designed to prevent forcible entries.

Burglary/Fire-Resistive Containers

Since 1975, special, single containers have been able to pass UL tests for both fire and burglary protection. A container may offer burglary resistance for either 30 minutes or one hour and either one-hour or two-hour fire protection. A typical container uses heavy insulation around the safe contents, leaving no voids for heat to penetrate. The body is made of high-tensile, electrically welded steel with doors of high-tensile and armor plate steel designed to resist attacks using power-driven carbide drills, abrasive wheels, and other burglary tools.

Because insurance underwriters give careful attention to the classification of security containers in establishing insurance premiums, this factor should be weighed before a container is selected. The purchase of the appropriate container can often result in a substantial benefit in the form of reduced premiums. In some cases, the annual premium savings can equal the cost of the equipment in a short time.

GSA-Approved Safes

Although not specifically designed to protect valuables, six classes of safes for protection against either forcible or surreptitious entry have been tested and approved by the U.S. General Services Administration (GSA) for the storage of government classified information. The standards are available at www.gsa.gov.

9.5 VAULTS

Vaults are specially constructed rooms or areas intended to limit access and provide protection to the assets in the space. Generally a vault is used to preclude forced entry and removal of the asset. The term *vault* also applies to specially constructed rooms or areas that are designed to protect the contents from fire and not necessarily theft. Compared to vaults designed to protect against theft, vaults designed to protect against fire are generally less expensive, follow very different construction standards, and provide much less protection from theft.

When deciding which standards to follow (those for fire or security), the owner must consider the asset being protected and its vulnerability. Another consideration is the legal responsibility and liability of the custodian to meet any special regulatory requirements or standards established by an insurance carrier or government agency.

9.5.1 FIRE-RESISTIVE VAULTS

The principal U.S. standard for fire-resistive vaults is National Fire Protection Association (NFPA) 232. The standard does not consider forcible entry.

A key issue is whether the vault will be located in a fire-resistant building. As defined in NFPA 220, Standard on Types of Building Construction, a fire-resistive building uses walls, partitions, columns, floors, and roofs of noncombustible or limited combustible material. The required degree of vault protection is greater in non-resistive structures.

Records of exceptionally high value or rarity might require individualized protection measures outside the scope of existing standards. Records essential to the reconstruction of other records should be receive special protection.

Vaults require unusually good design and construction to ensure that the structure withstands all the conditions that could be imposed on it by fire. One should avoid installing vaults below grade because under certain conditions burning or smoldering debris can accumulate in a basement to produce a long-lasting cooking effect that overcomes the vault's protective qualities. Also, vaults below grade might be damp, enabling mold to harm records, and may also be subject to flooding.

Traditionally vault construction meets these standards:

- **Reinforced concrete with steel rods at least 0.5 in. (13 mm) in diameter, spaced 6 in. (152 mm) on center and running at right angles in both directions.** Rods are wired securely at intersections not over 12 in. (305 mm) apart in both directions and installed centrally in the wall or panel.

- **A structural steel frame protected with at least 4 in. (102 mm) of concrete, brickwork, or its equivalent tied with steel ties or wire mesh equivalent to No. 8 ASW gauge wire on an 8 in. (203 mm) pitch.** Any brick protection used is filled solidly to the steel with concrete.
- **Fire resistance determined by wall thickness.** The minimum thickness of a 4- hour vault wall is 12 in. (305 mm) for brick and 8 in. (204 mm) for reinforced concrete. The minimum thickness for a 6-hour vault wall is 12 in. (305 mm) for brick and 10 in. (254 mm) for reinforced concrete.

9.5.2 **MEDIA STORAGE AND PROTECTION**

Magnetic media are often stored in the same vaults used for paper products. It is impractical and not cost-effective to construct the entire vault at a level that protects such media when most of the vault's contents do not require such special protection. It is better to place an additional container within the vault to protect such assets.

The following are some standards and ratings for media storage:

- American National Standards Institute (ANSI): ANSI IT9.11, Standard for Imaging Media—Processed Safety Photographic Film Storage
- American Society for Testing and Materials (ASTM): ASTM E 119, Test Method for Fire Test of Building Constructive Materials
- Factory Mutual Research Corporation (FM): FM Approval Class 4200, Storage of Records and Valuables
- National Fire Protection Association (NFPA): NFPA 232, Standard for the Protection of Records; NFPA 40, Standard for the Handling and Storage of Cellulose Nitrate Film Records; and NFPA 232AM, Standard for Fire Risk Evaluation of Structures Containing Vital Records. NFPA 75 Standard for the Protection of Electronic Computer/Data Processing Equipment
- Underwriters Laboratory (UL): UL 72, Test for Fire Resistance of Record Protection Equipment; and UL 155, Tests for Fire Resistance of Vault and File Room Doors.

9.5.3 VAULTS FOR PROTECTION AGAINST FORCED ENTRY

Protection for Vault Surfaces

An important consideration is the location of the vault. An exterior location is not desirable because an exterior wall might provide a convenient point for an individual to attack the vault surfaces from the outside.

Also, all six surfaces of a vault should give equal protection against forced entry. It would be a mistake to install a heavy door on an enclosure and assume that, because they appear to be rugged and formidable, the concrete walls surrounding the door are adequate. Although concrete may appear to give adequate protection against penetration, it is usually vulnerable to rapid penetration when modern tools are used. Such walls are normally designed to support structural loads, not to discourage or delay forced penetration. Concrete is brittle and has poor tensile as well as flexing properties; thus, it is relatively easy to penetrate.

Unreinforced concrete should never be used for protection against forced penetration. Steel reinforcing bars, referred to as rebar, are commonly used as reinforcement for concrete. Rebar is normally sized by number, the numbers representing multiples of 1/8 in. (3 mm) diameter. For example, a Number 3 would be a 3/8 in. (10 mm) diameter rebar. The current ASTM vault construction specification requires the use of rebar.

All surfaces of the vault are vulnerable to penetration. A vault will only delay, not stop, a determined intruder. It is impossible to construct a vault that cannot be penetrated. Vaults are designed to resist penetration for a defined period. Even the thickest, best-reinforced concrete is vulnerable to an intruder with the necessary skill, manpower, and tools.

Penetration Techniques

Explosives are particularly effective in penetrating concrete because the shock waves from an explosion propagate throughout, resulting in internal fragmentation and splaying of the inner as well as outer surfaces. Steel reinforcement increases the penetration delay because even though the concrete can be penetrated by an explosion, the reinforcing material usually remains intact. The steel reinforcing material must then be removed, requiring more time.

The size of reinforcing steel used has a significant effect on the protective qualities of a reinforced concrete surface. For example, Number 4 or smaller rebar can be cut with handheld, manually operated bolt cutters, while Number 5 to 8 rebar requires power-operated hydraulic bolt cutters, cutting torches, or burning bars. Rebar larger than Number 8 can only be cut with a torch, burning bar, power saw, or explosives.

Wall Construction and Penetration

One advantage of thicker reinforced concrete walls is that anyone attempting to make a penetration must use sophisticated tools and explosives. Also, more supplies, such as tanks of acetylene, must be provided to penetrate a wall. Because of the tool and supply requirements and the resulting noise, smoke, and heat, penetration must be made at a concealed location. There have been cases where a building near a bank was been leased and used as a front to tunnel into the bank and penetrate through the floor. In one instance, a gang leased a building across the street from a bank and spent considerable time tunneling under the street to reach the bank vault. However, the bank vault was alarmed, and as soon as floor was penetrated, the alarm sounded and the penetration was discovered.

Still, it may be difficult to isolate an attempted penetration through the floor of an alarmed vault if the vault is locked with a time lock, as is the case with modern bank vaults. Even if an alarm signals a penetration, it will be impossible to open the vault door until the programmed time. However, CCTV with audio and lighting, installed inside the vault, can permit observation and, if recorded, create a record of the intrusion.

Vault Vulnerability Considerations

Inadequate policies and procedures for opening and closing vaults are often the downfall of even the best-designed vaults. For example, the “two-man rule” for use of the combination lock is vulnerable. In one case, individuals not familiar with the locking mechanism, which is a three-position, dial-type changeable combination lock, thought the combination had four numbers; they were counting the opening index (the last number) as part of the combination. The organization gave the first two numbers to one person and the third and fourth numbers to another. However, there are really only three numbers in the combination, and the last number is the opening index. If the first person wanted to, he or she could probably determine the remainder of the combination in less than 40 attempts. Common practice calls for not setting the first and last number of the combination above 10 or below 90, and the gates on the locking wheels are two digits wide.

When a locksmith is not used to change the combination, and the directions to change the combination are not followed exactly, the lock can be opened by dialing the last number and rotating the dial to the opening index. This is a serious problem. It is a very simple mistake caused by not following the dialing sequence, and it causes the lock to be set on one number. A way to test this possible weakness is to have the vault custodian turn the dial three times to the left and stop on the third number, and then turn the dial to the right to the opening index. If the bolt of the lock opens, the combination is set on only one number, and it will be necessary to change the combination immediately.

An additional procedural error in the case described is that often both individuals stood at the vault door when the other was dialing his or her numbers, and could easily see the combination being dialed.

Another potential vulnerability is the escape mechanism, such as a handle or release inside the vault.

Finally, a reputable locksmith should periodically inspect the locking mechanism to

- perform routine preventive maintenance on the lock and door and
- inspect the lock to ensure that no unauthorized modifications have been made.

Vault resistance levels are invalidated by the installation of any door, ventilator, or other port whose manufacturer's installation instructions have not been followed.

9.6 SUMMARY

This chapter described various barriers that are used to delay the adversary during an attack. Most conventional barriers, such as fences, locks, doors, and barriers for windows, provide short penetration delay against forcible (and perhaps stealthy) attack methods that do not use explosives. Against thick, reinforced concrete walls and other impressive-looking barriers, explosives become a more likely method of penetration by the adversary. Ensuring that meaningful barriers are in effect at all times of the day and night may be difficult without adversely affecting normal facility operation. Often, the use of compensatory measures, such as additional security officers, is required to offset the decreased delay and increased risk encountered during certain operations, such as fire drills or maintenance by contract employees.

A barrier system can be configured or enhanced to provide effective delay times. For instance, the presence of multiple barriers of different types along all possible adversary paths should complicate the adversary's progress by requiring that he or she be equipped with a number of different barrier attack tools and skills. Placing barriers next to detection alarms should aid in assessing and responding to adversaries.

If the facility to be protected has not yet been constructed, barriers can be incorporated into its design. For example, placing the facility either underground or aboveground with massive overburden is an option that should be seriously considered. Using balanced design principles, appropriate detection systems, and response forces, a facility can be made highly

resistant to outsider and insider threats, and to the method of transportation used by adversaries (foot, land vehicle, or aircraft).

Consolidating assets into a single room or vault is one of the most effective ways to reduce response time and the cost of delay upgrades. Having assets scattered throughout a site requires the guard force to accurately assess the threat location and contend with the possibility of diversionary tactics by the adversaries.

Dispensable barriers, such as entanglement devices, and dispensable chemicals such as obscurants, irritants, and foams, offer significant potential for increasing adversary delay. These dispensable deterrents should be coupled with passive structural barriers to synergistically increase delay times. Also, conventional breaching techniques and equipment used by an adversary may be so ineffective that the adversary would choose not to continue attacking that barrier. Any activated dispensable barrier requires protection of the complete activation system to prevent or adequately delay disablement by an adversary. Finally, the use of safes and vaults as asset enclosures can protect certain high-value items and important records.

REFERENCES

- Kane, J. W., & Kodlick, M. R. (1983). *Access denial systems: Interaction of delay elements*. SAND83-0362. Albuquerque, NM: Sandia National Laboratories.
- Kodlick, M. R. (1978). *Barrier technology: Perimeter barrier penetration tests*. SAND78-0241. Albuquerque, NM: Sandia National Laboratories. Available: <http://www.osti.gov/bridge/servlets/purl/6526792-TIdDTb> [2012, April 6].
- Nuclear Security Systems Directorate. (1987). *Access delay technology transfer manual*. SAND87-1926. Albuquerque, NM: Sandia National Laboratories.
- Sena, P. A. (1985). *Security vehicle barriers*. SAND84-2593. Albuquerque, NM: Sandia National Laboratories.
- White, I. B. (1981). *Explosive penetration of concrete walls*. SAND80-1942. Albuquerque, NM: Sandia National Laboratories.

Note: SAND documents may be obtained at <http://www.osti.gov/bridge/advancedsearch.jsp>.



PPS FUNCTION **RESPONSE**

The third and final primary function of a PPS is response. The response function includes responding personnel and the communications system they use. Chapter 10, Response, provides an overview of response principles and concepts. More information is available in the *Protection of Asset* volume on security operations.

CHAPTER 10

RESPONSE

10.1 SECURITY OPERATIONS

The composition of the response force varies from facility to facility. Part or all of the response force may be located on-site or off-site. The response force may include proprietary or contract guards, local and state police, and for some incidents, federal agencies such as the FBI, DEA, or Customs. In this text, *guards* will refer to the onsite personnel who are available to respond to an incident; *response force* is a more general term meant to include all security response personnel who may be involved in the response at a particular facility, both on-site and off-site.

Response may be broken into two major categories—immediate, on-site response (timely response) and after-the-fact recovery. Depending on the needs and objectives of a facility, it is prudent to decide in advance which type of response will be used at the site under various conditions. Protection of different targets may require different response plans. For example, stopping an intruder about to sabotage a critical valve in a refinery may require an immediate on-site response, while recovery may be a better technique for theft of low value company property. For a recovery-based response, the use of recorded video for after-the-fact review can be very effective and legally acceptable. In addition, after-the-fact recovery will likely use investigative tools. This subsystem of security is described in detail in the *Protection of Assets* volume on investigation.

Timely response requires better detection and delay than a response strategy that focuses on recovery of the asset. A recovery strategy may not be acceptable for all assets. For example, recovery of stolen documents or information may not be meaningful, because the thief may already have copied or distributed the information. In a like manner, once an incident of

workplace violence has occurred, the capture of the perpetrator is commendable; however, there is still the aftermath of the event to consider. This aftermath may include legal action by the victim or the victim's family against the facility, bad publicity for the facility, poor employee morale, and regulatory action against the facility.

Because of the wide variety of response force personnel, it is difficult to provide information concerning the specific procedures or tasks that the response force at a given facility may be expected to perform. Depending on the threat, consequence of loss of the asset, and the particular facility, the response force must either prevent adversaries from accomplishing their objective or work to recover the asset. Recovery efforts may include investigation of the incident to find the culprit, filing insurance claims, or pursuit of the adversary immediately after the incident. Specific task assignments to accomplish these functions will be reflected in variations of qualification standards, training requirements, and performance standards as measured by realistic tests, governed by policies and procedures at the facility.

10.2 GENERAL CONSIDERATIONS

Staffing of the response force is fundamental to the performance of the response function. Proprietary guard forces are those in which the members are direct employees of the facility. Contract services also exist for facilities that prefer to contract this service out to others. There is considerable debate as to which of these two options is best at a facility (Fisher & Green, 1998). It is likely that the answer will depend on the goals and objectives of each corporation and facility. Facility size, assets, location, cost, and other factors may favor use of one system over the other. Many facilities use a combination of the two, which can provide flexibility. In addition to the use of contract and proprietary guards, some facilities also hire members of local law enforcement to help at night or at periods of heavy demand, such as morning or evening rush hours. Use of local law enforcement officers is appealing because these officers have the legal authority to arrest or detain suspects and to use appropriate force.

Regardless of which type of guard force is used at a facility, the key to effective guard use is training. Hiring contract forces may reduce costs, but it does not absolve the hiring facility from responsibility for its actions. For this reason, it is important to provide training at the facility or to incorporate training expectations into the terms of the contract with the vendor. Hertig (Considering, 1999) has written about the considerations of contract versus proprietary forces. In addition to the use of contract and proprietary guards, some facilities also hire members of local law enforcement to assist at night or at periods of heavy demand, such as morning or evening rush hours. Use of local law enforcement officers is appealing because these officers have the legal authority to arrest or detain suspects and to use appropriate force.

The details of the legal issues associated with guards and the response force are too numerous and complex to be fully addressed here. Readers should consult the legal issues volume of *Protection of Assets* for more details.

The issues generally fall into the categories of civil and criminal law and liability. Under civil law, intentional torts such as assault, battery, false arrest and imprisonment, defamation, invasion of privacy, malicious prosecution, and negligence are common. Criminal law is pertinent when dealing with trespassers, illegal drug use, sexual assault, receiving stolen property, and fraud. In these cases, the guard force may need to collect evidence to present to law enforcement officers for further legal action. Another applicable area of law is labor law. Labor law addresses issues such as wrongful termination, activities by labor unions, and strike surveillance. Consideration of these legal issues and others is required to protect the corporation and its employees from legal action. Because each state and country has different laws concerning these issues, local law enforcement or attorneys should be consulted for guidance in establishing procedures. Hertig (Legal, 1999) has written an excellent overview of legal issues and the security function. In addition, some actions, such as kidnapping, require notification of federal agencies, which will then have legal jurisdiction. This principle also applies to bombings at private facilities or attacks on government property.

10.3 **CONTINGENCY PLANNING**

Contingency planning is an important part of a facility's ability to successfully resolve an incident. Prior planning helps a facility manager identify potential targets, respond to different threats, interact with outside agencies, and determine what level of force guards can use in various situations. Well-documented procedures should be developed in advance as a major part of contingency planning.

A critical part of the design and analysis process of a PPS is the identification of assets, addressed in Chapter 1, Problem Definition. Once assets are identified at a facility, the security manager can evaluate the likely routes an adversary might use to approach the facility boundary and the specific asset. This information will assist managers in developing detailed tactical plans to address various threats to the facility. In addition, it will be useful in determining guard patrol routes and schedules. Based on the adversary goal and the consequence of loss of the asset, different response force strategies will be used. These strategies include containment, denial, and occasionally assault.

Containment is the strategy used against an adversary with theft as the goal. Containment is the ability of the guards and the response force to prevent the adversary from leaving the site

with the stolen asset. A denial strategy is used when the adversary goal is sabotage or violent attack. In this case, the guards or response force must prevent the adversary from completing the task of sabotaging equipment or carrying out the violent attack on another person. It should be apparent that for a denial strategy to be successful, the response force must be present at the location and time of the sabotage or attack. A containment strategy for a sabotage goal does no good, because the response will come after the sabotage event has been completed. On occasion, the response force may need to use force to overcome an adversary. This is most common in hostage incidents or when dealing with mentally unstable individuals.

Tactical planning should also be part of contingency planning in general. Procedures and plans for guard actions in the event of an adversary attack should be well established. The chain of command and the succession of command in case of emergency should be well known. Plans must be made to ensure that members of the response force possess or have rapid access to the proper equipment consistent with the defined threat. Tactical plans must contain specific details for the response force to deploy successfully. The response strategies of containment, denial, and assault must be well planned and practiced.

The role of the guard force should also be factored into the facility contingency plan. A guard force whose key role is the containment of adversaries until additional help arrives will deploy differently than a guard force capable of recovery operations. It is possible that there will be two sets of guards at a facility—one group checking credentials, patrolling, and serving the deterrence/delay role, and another, more highly skilled group with primary responsibility for response to a malevolent event.

Security managers should consider using support from outside agencies as they do their contingency planning. A facility may create support agreements with local or state law enforcement agencies or mutual aid agreements with other local sites. To facilitate this, a written support agreement with outside agencies or sites should be developed. This written agreement should detail the interaction between guards and these agencies. The agreement should be developed with input from all participants affected by the agreement and approved by each organization. Issues such as the outside agency's role in an incident, off-site pursuit by guards, and communication should be considered. The roles of outside agencies should be well defined and communicated among all participants. Security managers may also consider use of other agencies for recovery support. These decisions will need to be based on the agency's response time, training, equipment, and availability to support the facility. In addition, security managers may decide to provide their guards with off-site credentials and authority to facilitate the response force's ability to operate outside the facility's boundaries. This may be an important consideration during deployment or pursuit.

Security personnel, due to their access and familiarity with a facility, are a natural choice for assistance under abnormal conditions at a site. The facility may ask security personnel to help in the event of a natural disaster, bad weather, or accident. These services are reasonable but should not be allowed to compromise the protection of assets at the facility. Procedures should be determined in advance with facility safety personnel, management, legal counsel, local law enforcement, and other public safety agencies. These procedures should be documented and included in guard training. Part-time peace officers working at the facility should also know about these procedures and any hazards that exist at the facility. These procedures do not need to be specific to each abnormal condition, but can be used as applicable. For example, in case of bad weather, the procedure may require early arrival of facility maintenance personnel to place rugs at doorways to prevent slipping or other site preparation measures, such as snow removal. The procedure may also include notification to employees of a delayed work schedule announced via local radio, employee voicemail, or through a hot line. The guard force should be aware of these procedures and understand their role at these times. In the event of a power failure or a fire, security personnel may be used to assist in evacuation of buildings and crowd control until the “all clear” is issued or another determination made. These procedural elements can then be applied as needed for a particular emergency. The security manager alone cannot create these procedures; rather, they require input from various components of the facility.

In addition, natural or man-made disasters that cause business at the facility to cease may also require the help of the security organization. If the stoppage is due to an adversary attack, the company must have processes and procedures in place to resume operation as soon as possible, while still collecting and preserving evidence. In the event of an abnormal incident, use of daily operational procedures, such as daily backup of computer files or storage of backup records at an off-site location, may reduce the effect of a catastrophic event. The security organization can play a role in helping the facility get back to normal operation after an abnormal event, and certainly will be involved in investigation of any malevolent events and their aftermath. Abnormal conditions may reveal weaknesses in the security protection at a facility and provide an opportunity to improve asset protection.

Communication will be a key factor in the interaction between facility personnel and other agencies. Since different agencies may not operate on the same radio frequency, the security manager will need to evaluate alternate means of communication during abnormal or malevolent conditions. A dedicated land-line may be used for initial notification to outside agencies, and pre-planned routes and containment positions may help resolve on-scene communications concerns. For a deeper understanding of response and contingency planning, see the *Protection of Assets* volume on crisis management.

10.4 PERFORMANCE MEASURES

Various measures can be used to evaluate an immediate response to a security event. One measure is the time it takes for guards to arrive at the correct location. Another is the probability of communication, which includes transmission of an alarm to a monitoring location, assessment of the alarm, and contact among guards or other responders as they deploy to their assigned locations.

Other measures of response effectiveness include interruption and neutralization. *Interruption* means the arrival of response personnel at a location to stop the adversary from progressing in the attack. Interruption may be accomplished by one person or several; for example, arrival of one person at a location may be enough to scare away teenage vandals, but more motivated threats may require more responders. For low to medium threats, interruption alone may be enough, but for medium to high threats, neutralization of the adversary may be necessary. Interruption depends on reliable, accurate, fast alarm reporting and assessment, along with reliable communication and effective deployment to the proper location.

Neutralization refers to defeat of the adversary by responders. Some threats require more than a mere response presence if they are to be defeated. Neutralization elements include response tactics, procedures on issues such as use of force and post-detainment actions, training, the number of personnel who respond to the alarm, and the equipment they carry. Neutralization may use the entire force continuum, from presence, verbal commands, and physical restraint to intermediate force weapons such as batons and pepper spray to deadly force (at some high-security locations). The response force must be at least equal to the adversary in terms of equipment, weapons, and number if it is to successfully neutralize the adversary.

An additional factor in response effectiveness is guard fatigue. Miller (2010) summarizes guard fatigue issues (e.g., human-machine interaction, decreased performance from cognitive failure, and means of quantifying fatigue effects), and he discusses ways of mitigating fatigue effects. One solution is smart scheduling, which is based on these principles (Miller, 2010):

- **Principle 1: Shift lag.** Use a shift plan that maintains human circadian entrainment to the local, 24-hour light/dark cycle. Usually, rapidly rotating plans are better at this than slowly rotating plans.
- **Principle 2: Shift length.** Use a shift length of no more than eight hours, with the exception of using a 12-hour shift length for jobs with low physical and emotional work stresses.

- **Principle 3: Night shifts.** Schedule a minimal number of consecutive night shifts in the shift plan, preferably no more than three in a row.
- **Principle 4: Recovery.** Schedule 24 hours of recovery (not “time off”) after each night shift.
- **Principle 5: Weekends.** Schedule the maximum number of free days on weekends.
- **Principle 6: Days off.** Schedule at least 104 days off per year (equal to 52 weekends).
- **Principle 7: Equity.** Provide all workers with equal demands for long duty days, night work, and weekend work, as well as equal access to good-quality time off and weekends off.
- **Principle 8: Predictability.** Ensure that the schedule is so easy to understand that workers may apply simple arithmetic to predict their actual work and free days well into the future.
- **Principle 9: Good-quality time off.** Schedule long, contiguous periods of time off; operationally, this translates into three or more consecutive days off.

REFERENCES

- Fischer, R. J., & Green, G. (1998). *Introduction to security*, 6th ed. Boston: Butterworth-Heinemann.
- Hertig, C. A. (1999). Considering contract security. In S. J. Davies & R. R. Minion RR (Eds.), *Security supervision: Theory and practice of asset protection*. Boston: Butterworth-Heinemann.
- Hertig, C. A. (1999.) Legal aspects of security. In S. J. Davies & R. R. Minion RR (Eds.), *Security supervision: Theory and practice of asset protection*. Boston: Butterworth-Heinemann.
- Miller, J. C. (2010). *Fatigue effects and countermeasures in 24/7 security operations*. CRISP report. Alexandria, VA: ASIS Foundation.

SUMMARY OF PART II

PHYSICAL PROTECTION SYSTEM DESIGN

Part II, containing Chapters 2-10, described the functions of a PPS in some detail. The primary functions of a PPS are detection, delay, and response; deterrence is a secondary function. Deterrence is the first layer of defense of a PPS and can be effective against some threats. The detection subsystem includes sensors, video, alarm communication and display, and entry/access control. Each of these components combines people, procedures, and technology to provide notification of a potential security event. The difference between video surveillance and video assessment was also described, the major difference being the use of sensors to trigger an event and the immediate presentation of pre-and post-alarm video to a human operator for immediate action. The alarm monitoring system must communicate a sensor activation to a central monitoring point, and then appropriate data is displayed to the operator. Tight integration of technology, human factors, procedures, and training is required to make the alarm monitoring system as effective as possible. Another element of the detection subsystem is the entry/access control system, which controls the passage of people and materials into and out of a site.

The next function of the PPS is delay, where adversary progress is slowed down in order to allow more time for the appropriate response after detection. This subsystem uses structural or dispensable barriers, in conjunction with vehicle barriers, and guards to delay adversaries. In addition, safes and vaults are types of asset enclosures which add delay against adversaries.

The final function of a PPS is response, which was generalized as falling into two categories—immediate on-site and delayed after-the-fact. An immediate on-site response is required to protect critical assets, while a delayed response may be more appropriate for lower-value assets. Response strategies including containment, denial, and occasionally, assault (or force) were described. Contingency planning is a major aspect of response and must be carefully considered by the security manager to be sure that the response plan provides the desired performance. After a PPS is designed, the next step is to evaluate the design for its effectiveness in meeting protection goals and objectives. That is the subject of the next aspect of physical protection systems, analysis.

PART III

ANALYSIS

Part I of this book examined physical protection system goals and objectives. Part II addressed physical protection system design, looking at numerous principles, measures, and tools for securing a site. Part III discusses the issue of analysis, presenting various tools for determining the effectiveness of a physical protection system.

Part III presents its discussion in Chapter 11, Analysis of the Physical Protection System.

CHAPTER 11

ANALYSIS OF THE PHYSICAL PROTECTION SYSTEM

11.1 INTRODUCTION

At this stage, the objectives of the physical protection system have been established, and a new or upgraded design has been developed. The next step is to analyze how effective the design will be in meeting the objectives. This chapter examines the process of analysis, the evaluation of the PPS compared to threats and asset value (not the overall risk analysis that is also done). Risk assessment was described Chapter 1, Problem Definition.

Analysis evaluates whether the PPS's people, procedures, and technology are achieving the PPS functions of detection, delay, and response. This evaluation, also called a site survey or vulnerability assessment, may be qualitative or quantitative.

A qualitative analysis applies in evaluations of lower-security applications. Such facilities have lower consequence loss assets and can better withstand loss of or damage to an asset. Examples include retail stores, apartment buildings, small businesses, and restaurants. Some sites have a mix of assets, requiring the PPS designer to provide the most protection to critical assets and less protection to other assets. Other constraints may affect the protection system design, too. For example, despite tragic school shootings, it would be inappropriate to turn schools into armed camps with many layers of security surrounding them. The system's design and implementation depend greatly on the facility's goals and constraints.

For assets with unacceptably high consequence of loss, it is necessary to conduct a rigorous quantitative analysis, even if the probability of attack is low. Sites meeting this description include commercial nuclear power plants, prisons, and certain government or military installations. In some cases, the category would also include museums, refineries, utilities, airports, telecommunications hubs, and large industrial complexes. These are sites where

loss of or damage to certain assets can have high consequences—loss of many lives, loss of an irreplaceable piece of culture or history, damage to the environment, or compromise of national security. The response strategy for these assets is usually an immediate on-site response. A quantitative analysis is only justified if the asset needs this level of protection and performance measures for system components are available.

Analysis of the PPS provides two key benefits:

- It establishes the assumptions under which a design was formed.
- It relates system performance to threats and assets, making possible a cost-benefit decision.

Whether a qualitative or quantitative analysis is used, proper application of the system concepts and principles described in the previous chapters will assure the effective protection of assets at a facility. A key principle of analysis is that an initial baseline must first be established; upgrades are then considered if the baseline shows that the PPS does not meet goals and objectives.

A PPS is a complex configuration of detection, delay, and response elements. Analyzing them points out system deficiencies, helps in evaluating improvements, and facilitates cost-versus-effectiveness comparisons. One can analyze an existing protection system or a proposed system design. An existing protection system should be reviewed and updated periodically to take account of advances in protection hardware and systems as well as new processes, functions, or assets at the facility. Moreover, changing circumstances (such as threat escalation) call for PPS design changes over time. Periodic reanalysis makes it possible to gauge the effect of these changing conditions.

11.2 ANALYSIS OVERVIEW

Two basic analysis approaches are used in a vulnerability assessment (VA)—compliance-based and performance-based. Compliance-based approaches depend on conformance to specified policies or regulations; the metric for this analysis is the presence of specified equipment and procedures. Performance-based approaches, on the other hand, evaluate how each element of the PPS operates and what it contributes to overall system effectiveness. As discussed in Chapter 1, Problem Definition, the use of compliance-based (or feature-based) systems is only effective against low threats, when assets have a low consequence of loss, or when cost-benefit analyses show that physical protection measures are not the most cost-effective risk management alternative. A compliance-based analysis is

easier to perform because the measure of system effectiveness is the presence of prescribed PPS equipment, procedures, and people. The analysis consists of a review of facility conformance to the compliance requirements, the use of checklists to document presence or absence of components, and a deficiency report that notes where the facility is out of compliance. The VA report summarizes these findings and the facility makes improvements according to enterprise policy.

Although qualitative and quantitative analysis techniques are discussed separately, both approaches can be used in a performance-based analysis; the unique aspect of quantitative analysis is the use of numerical measures for PPS components. Even a quantitative analysis has qualitative aspects, but by using quantitative performance measures for PPS elements, particularly hardware, much of the subjectivity of compliance-based and qualitative analysis approaches can be removed. A quantitative approach is not applicable to every facility, but it certainly is for critical or unique assets, and since the attacks of 9/11 there is greater interest in applying this approach to critical infrastructures or national security assets.

Qualitative analysis should be based on the application of the first principles of physical security to verify the effectiveness of installed protection elements (equipment, people, and procedures). A few of the most critical principles are reviewed below. System effectiveness is a result of proper implementation of these principles:

- **Detect an adversary attack while there is still enough time to respond as desired (timely detection).** Detection elements are best early on the path, while delay is best later. If initial detection occurs at the asset, the PPS is fundamentally flawed.
- **Provide a timely and accurate assessment of alarms to separate valid intrusions from nuisance alarms.** The frequency of nuisance alarms should be low to maintain high system effectiveness. The best alarm assessment technique is the use of rapid and automatic display of video showing sensor alarm sources.
- **Communicate alarm information to a response force in a timely manner, or record all required information for after-the-event response.**
- **Establish performance measures for each PPS function—detection, delay, and response—for each defined threat category or level.** Estimates must be made considering all facility states, such as bad weather, varying operational conditions, and emergencies.
- **Ensure detection occurs before delay.** Detection is not complete without assessment, and delay prior to or without detection does not contribute to overall system effectiveness.
- **Delay the adversary long enough for alarm recording and storage or for immediate response to interrupt the adversary.**

- **Use protection-in-depth (multiple layers).** Protection-in-depth allows more opportunities to defeat the adversary, requires more planning and capability by the adversary, and avoids single-point failures. (An example of a single-point failure is the presence of only one layer, with an exploitable weakness). In essence, if there is one weakness in a layer, the layer is vulnerable and will require an upgrade.
- **Ensure balanced protection.** Balanced protection verifies that all paths to assets have approximately the same effectiveness. Balance should be maintained within each layer and under all facility states. If balance is not supported, system effectiveness will be reduced.
- **Engage and neutralize the adversaries, using force if appropriate.**
- **Conduct path and scenario analyses, and use analysis tools to predict system effectiveness, using interruption alone, or in combination with neutralization, as the overall performance measure.** There are many paths into a facility and the most vulnerable path is the one with the lowest effectiveness. Therefore, analysis characterizes the overall effectiveness of the system in detecting, delaying, interrupting, and neutralizing the defined threat along all credible paths.

A quantitative analysis also applies these principles, but uses numerical estimates, such as probabilities and delay or response times, to represent their application. While this approach is more objective, it is not mathematically rigorous. However, characterizing technology by testing to statistical standards is still the best technique to objectively assess security elements and systems. The testing process allows data to be collected by considering attack techniques (walking, crawling, bypass, spoofing, etc.) and the effects of weather, installation, operation, and maintenance on the device. Testing provides insight into the best performance expected from a given device for a given threat and serves as the basis for application of degradation factors that are used in VA analysis.

11.3 ANALYSIS TOOLS

Several tools can be used in analyzing a PPS. Some are software-based, while others are simple paper-and-pencil approaches. One simple path analysis computer tool is available at <http://www.elsevierdirect.com/companion.jsp?ISBN=9780750683524>. Many large enterprises have proprietary software tools that aid in collecting and documenting VA information and automate the analysis process. The key to using analysis tools is to understand that they are only tools—the analysis still depends on the appropriate interpretation of data by the VA team. It is not sufficient to purchase or develop a software tool and then defer to it for results. It is imperative that knowledgeable people interpret tool results and draw the proper

conclusions. In addition to complex (and often very expensive) commercial software tools for security data collection and analysis, there are also simple tabletop models for capturing and representing aspects of physical security at a facility. Investigative tools used to support analysis include timeline analysis (the sequence of actions that have been described by witnesses or supported by evidence) or investigative management software that allows for incident information to be entered into a system and shared by investigators.

This chapter focuses on two tools that support analysis—CARVER+Shock and Adversary Sequence Diagrams (ASDs). CARVER is a targeting tool originally developed by the U.S. government during World War II. An ASD—a functional representation of a facility and asset locations—is an aid in path analysis. Either or both of these tools can be used in an analysis. The choice is often a matter of enterprise policy or proficiency in specific tools. Checklists, a commonly used qualitative analysis tool, were described previously in Chapter 1, Problem Definition.

11.3.1 QUALITATIVE ANALYSIS—CARVER

As noted above, CARVER was developed by the U.S. government as a targeting tool. It was provided by the Office of Strategic Services (predecessor to the CIA) to resistance groups working behind enemy lines to select the best targets for attack. In 2003 it was declassified and since then has enjoyed a resurgence in use. CARVER is an acronym for the following six attributes used to evaluate the attractiveness of a target for attack (Food and Drug Administration, 2007, p. 2):

- **Criticality:** a measure of public health and economic impacts of an attack
- **Accessibility:** ability to physically access and egress from target
- **Recuperability:** ability of a system to recover from an attack
- **Vulnerability:** ease of accomplishing attack
- **Effect:** amount of direct loss from an attack as measured by loss in production
- **Recognizability:** ease of identifying target

A modified CARVER tool evaluates a seventh attribute, the combined health, economic, and psychological impacts of an attack, or the shock attributes of a target, considered on a national level (Food and Drug Administration, 2007, p. 7).

CARVER applies a multi-step process to subjectively evaluate an asset as a target of attack by an adversary, from an adversary's perspective. The steps include establishing scenarios and assumptions, assembling a team of experts, describing the system to be evaluated, and assigning scores to the seven attributes (Food and Drug Administration, pp. 3-4). The tool

can be used when performing a VA, as it quickly helps in determining assets that may be attractive to adversaries. However, according to Cummings et al. (2006):

CARVER works best when comparing assets that either share a mission or are in the same infrastructure and does poorly otherwise. CARVER's simplistic net scores lose valuable information about individual scores, and implementing CARVER is fraught with subjective decisions that may produce inconsistent results. Finally, when changing the above criteria, one must carefully do so in a way that avoids double counting when scores are summed.

In addition, using a scenario-based approach has some drawbacks, as described in Chapter 1.

11.3.2 PERFORMANCE-BASED ANALYSIS

When conducting either a qualitative or quantitative performance-based analysis, the same six-step process is used. The steps are these:

1. Create an adversary sequence diagram (ASD) for all asset locations.
2. Conduct a path analysis.
3. Perform a scenario analysis.
4. Complete a neutralization analysis, if appropriate.
5. Determine system effectiveness.
6. If system effectiveness (or risk) is not acceptable, develop and analyze upgrades.

As described in Chapter 10, Response, *interruption* is defined as arrival of responders at a deployed location to halt adversary progress. Interruption may lead to neutralization. Neutralization is the defeat of the adversaries by responders in a face-to-face engagement. The probability of interruption (PI) and the probability of neutralization (PN) are the performance measures used for these elements. These probabilities are treated as independent variables when the defined threat selects a path that exploits vulnerabilities in the PPS and is willing to engage with responders. In this case, physical protection system effectiveness (PE) is calculated by this formula:

$$PE = PI \times PN$$

Some adversaries may not be violent and will give up when confronted by any immediate response; therefore, PN is not a factor. In other cases, there is no immediate response, so PN may not be a useful measure of system effectiveness. Under these conditions, PE is equal to PI. If desired, a facility may also evaluate the PPS using risk as a metric, although this method is more commonly used in risk assessment and not in vulnerability assessment. The risk equation was described in some detail in Chapter 1, Problem Definition.

In a qualitative performance-based analysis, one uses designators like high, medium, and low to represent interruption, neutralization, and system effectiveness. These values are estimated by the VA team, using component performance estimates and applying the security principles described above.

11.3.3 ANALYSIS PROCESS

This section describes the performance-based analysis process at a high level and describes how qualitative or quantitative techniques can be used for a performance-based evaluation. The analysis and evaluation principles and models used here are based on the existence of adversary paths to an asset. An adversary path is an ordered series of actions against a facility, which, if completed, results in successful theft, sabotage, or other malevolent outcome. Insider analysis is similar but eliminates some layers of protection due to their authorized access to at least some areas of a facility.

An adversary sequence diagram (ASD) is a functional representation of the PPS at a facility that is used to describe the specific protection elements present. It illustrates the paths that adversaries can follow to accomplish sabotage or theft. Because a path analysis determines whether a system has sufficient detection and delay to result in interruption, it is conducted first. The path analysis uses estimated performance measures, based on the defined threat tools and tactics, to predict weaknesses in the PPS along all credible adversary paths into the facility. This step is facilitated through the use of an ASD of the facility to be analyzed.

For a specific PPS and a specific threat, the most vulnerable path (the path with the lowest probability of interruption, or PI) can be determined. Using PI as the measure of path vulnerability, multiple paths can be compared and an estimate of overall PPS vulnerability can be made. The analyst may either construct the ASD manually using pencil and paper or create it electronically using software tools.

There are three basic steps in creating an ASD for a specific site:

- describing the facility by separating it into adjacent physical areas
- defining protection layers and path elements between the adjacent areas
- recording detection and delay values for each path element

A more detailed description of the creation and use of ASDs is provided in Garcia (2008, pp. 283-288). Caution should be used when creating an ASD. While the technique seems simple, it may be difficult to draw the ASD due to overlapping layers and unknown or undiscovered entry points, such as roof hatches, an elevator penthouse, or other sites overlooked when one does not view the facility as concentric layers. The biggest mistake is to follow a single path

from off-site to the target location and only do an analysis on that path. This approach obviously does not consider all the paths into the facility. The best method for creating an ASD is to walk or drive around the exterior of the area, then repeat do the same inside. This is supplemented by the use of site drawings showing overall site layout and specific interior building details.

The ASD represents adjacent areas of a facility using concentric rectangles, and it models a PPS by identifying protection layers between adjacent areas. The first layer is always off-site (i.e., off facility grounds), and the last layer is always the asset. Each protection layer consists of a number of path elements (PEs), which are the basic building blocks of a PPS. A key point in developing ASDs is that one ASD must be created for each asset (target location), unless the assets are co-located. At complex facilities, several critical assets may need protection, and ASDs should be developed for each unique location.

Once the ASD is created, the analyst assigns detection and assessment probabilities, delay times for PPS elements under different facility states, and any additional notes for each path element. The values recorded are the estimates provided by the VA team subject matter experts as a result of their evaluation. These estimates include the probability of communication and the response force time, when there is an immediate response. This is the initial step in path analysis. Both entry and exit path segments can be modeled. The entry path segment is from off-site to the asset, and the exit path segment is from the asset back off-site. A given path element may be traversed once, either on entry or exit, or it may be traversed twice, on entry and in the opposite direction on exit. The adversary attempts to sequentially defeat at least one element in each protection layer while traversing a path through the facility to the target. The ASD represents all adversary paths to an asset; paths that are not credible are identified in scenario analysis (next section). While only some paths are credible for specific threats, representing the entire PPS on the ASD is recommended. This provides good system documentation, allows for faster replication of analysis if threats increase, and facilitates sensitivity analysis (how well the system performs against higher or lower threats). This simple functional view also provides additional insights about credible adversary paths, which could be missed if some path elements are omitted.

For sabotage analysis, only entry paths are evaluated, and the assumption is that the path elements will be traversed in only one direction. This is because a successful act of sabotage only requires proximity to the asset long enough to cause damage; it does not require adversary exit from the facility. For theft analysis, the path elements are traversed twice—on entry and on exit from the facility. When only entry paths are considered, the total number of paths is the product of the number of protection elements in each layer. When both entry and exit paths are evaluated, the total number of paths is the square of the number of entry paths.

The path analysis is used to provide an overall view of the robustness of the PPS—whether the system has many weak paths or only a few. By studying the potential adversary paths and the estimates of path element performance, the analyst can quickly determine how effective the PPS is and where vulnerabilities exist. For example, if there is no detection along a path until the asset, this is quickly revealed. Path analysis also identifies element performance for multiple adversary paths. This information provides insights into common weak points along paths that need additional detection or delay to support the desired response. During path analysis, the assumption is that interruption and neutralization will occur in time to protect the asset, although the actual response strategy depends on the asset. For example, if the asset is a sabotage target using a denial strategy, the response must occur no later than at the asset; theft targets can use a containment strategy. When a facility has multiple distributed assets that are targets of different adversary attack goals (sabotage and theft), response must be carefully planned to support both protection goals. The key objective of path analysis is to evaluate the PPS at a facility at a high level and determine how well-protected all assets are at all times.

Reviewing the ASD during path analysis can also reveal whether the PPS is balanced or not. For each protection layer, the detection and delay provided by path elements should be balanced. Examining overall detection and delay values can quickly show unbalanced elements or layers that will be preferred in adversary paths. Verifying balance across protection layers will also assist if upgrades are required. If a layer is already balanced, upgrades must be applied to each protection element to maintain balance. If a layer is not balanced, upgrades should be applied so they bring the layer into balance.

It is likely that there will be at least two ASDs for each target—one each for the day/night or open/closed facility states. Depending on other facility states, more ASDs may be required. Examples of other facility states that deserve consideration include employee shift changes, guard force shift changes, fire or other emergencies, power failures, bad weather, and sensors in access mode during operational times. This process is not as onerous as it sounds. Once an ASD for a specific asset is drawn, successive views need only capture the changes from one facility state to the next. Analysis is often expedited by making several copies of the initial ASD, and then modifying only the path elements that change. Once these differences are understood, it is a simple matter to describe them in a short paragraph in the VA report. Analysis of the facility states should emphasize additional path vulnerabilities at these times.

Developing an ASD can also reveal whether a protection system is balanced. For each protection layer, the detection and delay provided by path elements should be balanced. Looking across the protection layer detection and delay values can quickly show weak elements that will be preferred in adversary paths. Looking at balance across protection layers will also assist in looking at upgrades. If a layer in need of upgrades is balanced,

upgrades must be applied to each protection element to maintain balance. If a layer is not balanced, upgrades should be applied to bring the layer into a balanced state.

Scenario Analysis

Analysis of the ASD will identify the paths with the lowest PI, which is the starting point for scenario development and analysis. A scenario analysis is conducted to determine whether the system has vulnerabilities that could be exploited by adversaries using varying tactics, resulting in lower effectiveness of the PPS. Some facilities use scenario analysis as a substitute for a defined threat, where they postulate attacks, then decide what equipment or capability is required to be successful. This is another option, but it can lead to some gaps in analysis. Analyzing the PPS using defined threats and path analysis, and then generating scenarios by looking at weak paths, is the preferred approach to be sure no credible paths are missed. Using the scenario, a task-by-task or layer-by-layer description is developed. This description should be detailed enough to provide a scenario timeline and enough information that performance estimates for sensing, assessment, communication, delays, and response can be made.

At this point the analyst reduces all the possible paths to those that are most credible. Paths can be removed from the final mix due to a number of tactical issues. For example, a path that appears very weak (low PI) using element performance measures may not really be credible because there are a large number of responders on the other side of the door with the shortest delay. In another instance, the adversary might use one entry door instead of another because it is located in an isolated corner of the facility, even though both doors have the same delay. In reality, an adversary would select the door that gave the greatest chance of successful entry, assuming a similar delay time. Of course, some paths will be eliminated because the adversary does not have the equipment or other capability to attack some protection elements (for example, thick walls and only hand tools).

Once the path analysis is complete, scenario analysis begins. The steps to conduct a scenario analysis as follows:

- Develop attacks and tactics designed to exploit weak paths. Consider attacks during different facility states using the defined threat and capability.
- Modify performance estimates for path elements using these tactics or under these states.
- Document the assumptions used and the results of the scenario analysis.

A scenario analysis is aided by the creation of adversary task timelines and the associated performance of any path elements along the path. Scenario analysis considers specific tactics along the path, as well as attacks on the PPS itself or on the response force. These tactics

include stealth, force, and deceit, and they may be used individually or in combination during a scenario. For example, a VA team might determine that adversaries could easily jam radio communications at the facility. Evaluation tests indicate that an additional five minutes, on average, is required by responders to communicate using alternate means during jamming attacks. This time would be added to the response time used in the path analysis to evaluate how PI changes. Other attacks on the system might include interference with alarm transmission, disabling the alarm monitoring center, or shining bright lights into cameras. Examples of attacks on responders might include overt or covert attacks on patrols, diversions, or ambush during deployment. Other aspects of scenario analysis include consideration of what on-site tools or other equipment might be used by the adversary to aid in the attack. For example, forklifts, explosives, cutting torches, ladders, or power tools might be available at the facility. In this case, the adversary would not need to bring this equipment, and the scenario analysis would add procuring these items to the adversary tasks that must be completed for success.

In addition to the adversary task times, immediate response times must also be determined, if appropriate. The response time depends on the specifics of attack timing and response procedures, but a general notion of how many responders will respond to the area and at what intervals is an effective first step in response time estimates. The time for alarm assessment information to be relayed to responders is included in response time. Also, the ability of responders to engage from various locations, such as initial positions, while in transit, and at their deployed positions should be considered.

If one adversary tactic is to eliminate responders, scenarios are developed in which the attack begins by assaulting them. Because PI calculates the likelihood of arrival of the response force, and confrontation with the adversary is assured in this case, the PE is equal to the probability that the response force wins this confrontation (which is PN). It is important for the analyst to work closely with the VA team's subject matter expert on response during this stage of the analysis, so that the most credible paths of attack and realistic tactics are considered. As a result of this analysis, modifications are made to the path model that show changes in performance values that reflect these more realistic attacks. This stage of the analysis broadens the path analysis to consider attacks on PPS devices or the response force, in addition to direct attacks on the asset.

Scenario analysis also considers response to attacks on multiple distributed assets at a facility. If the facility has assets that are both theft and sabotage targets, the response to attacks must be carefully considered. During the early stages of an attack it may not be apparent which asset is the attack target. In these cases, the response team may have to wait until this is clear, or there must be enough responders to implement both denial and containment strategies. During scenario analysis, these attacks and their responses can be considered, and the ability to protect all assets under varying attacks can be evaluated. This

is a good example of the use of response storyboards or sand tables (enactment tools, described later), which can be used to show the inadequacy of response to multiple simultaneous attacks or different individual attacks, including theft and sabotage. In addition, scenario analysis may consider the neutralization effectiveness of an immediate response at various points along the adversary path. In this case, it is assumed that interruption has occurred, and the goal is for the facility to understand how many responders can get to a specific point on the path and their effectiveness after arrival at this point. This analysis provides additional insight into system vulnerabilities, and potential improvements to the overall PPS, especially response tactics.

At most facilities, only one threat team is considered; however, at some high-security facilities, it is very likely that the adversary will split into multiple teams, each with a separate task. One team will likely still be dedicated to attacking the asset. A table of scenario tasks and task times could be completed for each team, but it is more straightforward to complete a timeline for the asset attack team only, with the effects of other teams rolled up into sensing or assessment values or decreased response effectiveness. It is unlikely that force scenarios such as this will be used during the VA of an industrial facility.

As in path analysis, an important aspect of scenario analysis is consideration of different operating states at the facility or near the asset. There are usually at least two facility states—open and closed. For example, a door may be left open during daytime operation but kept locked at night. A good analysis will include scenarios predicting performance under both conditions. Even for facilities that operate 24/7, there may be differences among shifts, and these should be analyzed to verify that protection is balanced across all shifts. In addition to open and closed differences, there may be other predictable operating states at a facility, including safety emergencies, maintenance activities, bad weather (particularly for exterior PPS components), and power failures. Each of these states can represent a new set of vulnerabilities for the asset, the PPS, or security guards.

As a part of scenario analysis, an effort is made to identify the worst-case attacks. While analysis is not limited to these situations, they are very useful because they define adversary attacks that test the limits of PPS effectiveness. The worst-case scenarios are generally used in neutralization analysis since they predict the lowest response effectiveness. Although it is important to determine the worst-case scenarios, other less severe but more credible scenarios are also created and evaluated. These scenarios are then used in path analysis to calculate PI, and also to estimate PN, which is the other term needed to establish PE.

Estimate Neutralization

After weak paths and suitable attack scenarios have been determined, a neutralization analysis can be performed. This part of the analysis is only performed at facilities where there

is an immediate response resulting in any face-to-face confrontation with adversaries. Neutralization may take many forms, ranging from presence to deadly force (i.e., the force continuum). Neutralization analysis provides information about how effective the response will be under different attack scenarios and is a measure of response force capability, proficiency, training, and tactics. This analysis assumes that interruption has occurred. If the defined threat for an asset or facility includes adversaries who will use force to prevent the response force from interrupting or neutralizing, analysis should consider the likely outcome of that engagement. This analysis can use qualitative or qualitative techniques. At many high-security facilities, computer simulations are used to quantitatively predict the probability of neutralizing violent adversaries after interrupting them. For other facilities, PN can be estimated based on records of successful responses to security incidents or on tabletop exercises. In a qualitative analysis, the side that has the advantage—in numbers, weapons, skill, tactics, or other areas—can be determined and assigned a high, medium, or low likelihood.

Other Analysis

In addition to the analysis tools described above, other tools may be useful when analyzing the PPS at a facility. These include blast effects modeling, response storyboards, and sand tables. Many sites are specifically concerned about the threat of vehicle bombs or other explosive devices at critical locations at a facility. In these cases, it can be useful to provide some analysis of the effects of such a device on these structures. A number of commercially available blast effects modeling tools are available to support this part of an analysis. While some are not extremely robust, they do allow for a simple approximation of blast damage to buildings using standard construction. Inputs generally are simple and include the footprint of the building, building construction, size and location of the explosive charge, and surrounding terrain. The output is a graphic showing an approximation of blast damage. These images and supporting assumptions can be included in the final VA report.

Another useful tool, particularly during scenario analysis, is the response storyboard. A storyboard, resembling a series of cartoon panels, depicts where responders and adversaries are at periodic intervals. For example, the first panel might start at time zero and show the locations of each group; then every 30 or 60 seconds another “snapshot” could be captured. Through this technique insights may be gained for achieving faster or more effective responses. Creation of a response storyboard allows the analyst and tactical experts to get a sense of how long it will take for the response force to fully engage with the adversary and what tactics are appropriate at different stages of the attack and response. Often, the response storyboard is used for neutralization analysis and scenario development. A similar tool is a sand table, where responders and adversaries are shown using toy soldiers, which are moved around to show various approaches and tactics. These are often found at military installations or other critical asset facilities.

11.4 CALCULATE SYSTEM EFFECTIVENESS

At this point PPS effectiveness can be calculated, using the qualitative or quantitative estimates described above. Either way, system effectiveness can be represented using only PI (as in the case of a delayed response using review of video and investigation, when mere presence of an immediate response will chase an adversary away, or when an adversary will surrender if interrupted), or through the use of both PI and PN (at sites where an immediate response will engage with the adversary). If only PI is used, analysis will consist of path analysis and limited scenario development to support the estimate of system effectiveness. When both interruption and neutralization are used, system effectiveness is the product of PI and PN. In a quantitative analysis, the two terms are multiplied to establish system effectiveness. In a qualitative analysis, the two terms are combined to represent the overall state of system effectiveness. Just as in a mathematical multiplication, if one term is low, the other term will be decreased to that amount, even if it is very high. For example, if PI is high and PN is low, PE will be low. In general, PE can be no higher than the lower of the two values and this is a good guideline for qualitative analysis. (For example, $0.9 \times 0.2 = 0.18$. Even if the product is rounded up to the nearest tenth, it is still the lower of the two numbers.) PE is calculated for each threat category, since it is expected that the same system will have varying performance for different threats.

11.4.1 UPGRADE ANALYSIS

If the baseline analysis of the PPS shows that the system does not meet its protection objectives, and therefore is vulnerable, the VA team can suggest upgrades to address vulnerabilities. Usually, these upgrades are not specific technical recommendations but functional improvements that can be achieved by increasing performance at certain locations. These recommendations are then passed to the upgrade design team to aid in its selection of appropriate improvements. For example, the team might suggest that an improved PD at a certain point or that additional delay at an asset will increase PE. In these cases, the analysis assumes an improved functional performance without identifying the specific sensor or barrier device, although the evaluation team believes this is an achievable goal. The upgrade options generally consider the interaction of detection, delay, and response features, as well as operational effects, life-cycle performance-cost trade-offs, single-point failures, reliability, quality, and maintenance of the security system.

The analysis is then repeated using these performance increases to estimate the overall increase in the ability of the system to meet its objectives. These results (which become new system requirements for upgrade designs) can be provided to security system designers, who will determine which specific equipment or other upgrades will provide the required performance. These specific design details are generally addressed in a follow-on activity to

the VA, often captured in a conceptual design project or phase. Once the analysis is completed, it is important to clearly present both the baseline and upgrade analyses to establish the need for improvements and show the return on investment in upgrades.

The upgrade analysis is also the appropriate time to consider and evaluate the effectiveness of contingency plans and equipment. Contingency plans are used for various reasons, including when PPS equipment is under repair or when the impacts (cost, schedule, operations, acceptability) of PPS equipment required to meet protection objectives are deemed to be too great. For example, if a facility cannot afford to meet the protection objectives for all threats at all times, temporary procedures or portable equipment could be implemented during high-alert periods. Whenever contingency plans are part of security protection plans under elevated threat conditions, they should be evaluated using performance estimates and analysis tools to ensure they will perform as required.

11.5 SUMMARY

This chapter described analysis of the PPS using both qualitative and quantitative techniques. In addition, PPS analysis may be compliance-based or performance based. Compliance-based approaches depend on conformance to specified policies or regulations; the metric for this analysis is presence of specified equipment and procedures. Performance-based approaches, on the other hand, evaluate how each element of the PPS operates and what it contributes to overall system effectiveness. Analysis should be based on the application of the first principles of physical security to verify the effectiveness of installed protection elements (equipment, people, and procedures). System effectiveness is a result of proper implementation of these security principles.

Two analysis tools, CARVER and adversary sequence diagrams, were described, and the technique of path analysis was explained. The chapter described the use of interruption, neutralization, and system effectiveness measures to establish a baseline, and it discussed the use of an upgrade analysis.

REFERENCES

- Cummings, M. C., McGarvey, D. C., Vinch, P. M., & Colletti, B. W. (2006). *Homeland security risk assessment, volume II: Methods, techniques, and tools*. Arlington, VA: Homeland Security Institute.
- Garcia, M. L. (2008). *The design and evaluation of physical protection systems*, 2nd ed. Boston: Butterworth-Heinemann.
- U.S. Food and Drug Administration. (2007). *An overview of the carver plus shock method for food sector vulnerability assessments*. Available: <http://www.fsis.usda.gov/PDF/Carver.pdf> [2012, April 18].

PART IV

IMPLEMENTATION

Part IV, Implementation, is the last stage in a process that began with Part I, Problem Definition, and continued through Part II, Physical Protection System Design, and Part III, Analysis. This final stage takes a detailed look at the steps involved in implementing a physical protection system. It discusses such issues as the basis of design, design criteria, design, procurement, installation, training, testing, and maintenance.

Part IV presents its discussion in Chapter 12, Implementation of the Physical Protection System.

CHAPTER 12

IMPLEMENTATION OF THE PHYSICAL PROTECTION SYSTEM

12.1 INTRODUCTION

At this point, the problem has been identified, the existing or proposed design has been considered, and PPS performance has been analyzed. The last stage of the process is implementation of a final design. Proper use and application of the integrated security systems design process is the most important element in the defense against dynamic threats and potential catastrophic losses. In other words, a fence used primarily to delay entry provides only one of the four elements of physical design, which are deterrence, detection, delay, and response. Typically, design and integration are performed to introduce and meld technological and physical elements into the overall asset protection program. When carefully and diligently followed, the process results in a fully integrated security program that blends architectural, technological, and operational elements into a flexible, responsive system.

Integrated security systems designs can address any number of security subsystems or elements to form a complete system. Particularly important factors in system design are the environment or unique needs of the facility. Anticipated threats, risks, vulnerabilities, and constraints all need to be taken into consideration to pinpoint the best solution.

This chapter provides an overview of the tasks and players involved in a security systems implementation project from initial inception through project completion and systems operation. The basic tasks of security systems implementation are as follows:

- planning and assessment to determine security requirements
- developing conceptual solutions for resolving vulnerabilities
- preparing security systems design and construction documentation

- soliciting bids and conducting pricing and vendor negotiations
- installing, testing (which is most likely to be overlooked), and commissioning the security systems

This chapter focuses on the last three tasks. A system in the security context is a combination of equipment, personnel, and procedures, coordinated and designed to ensure optimum achievement of the system’s stated objectives. A system includes more than hardware components. A protective system is evaluated on the performance and cost-effectiveness of individual measures in countering threats, reducing vulnerabilities, and decreasing risk exposure considered as an integrated whole. Although much of the following discussion is related to security technology, the process also applies to the design, procurement, and deployment of other security elements.

12.2 SYSTEMS DESIGN PROCESS

Figure 12-1 provides an overview of the systems design process.

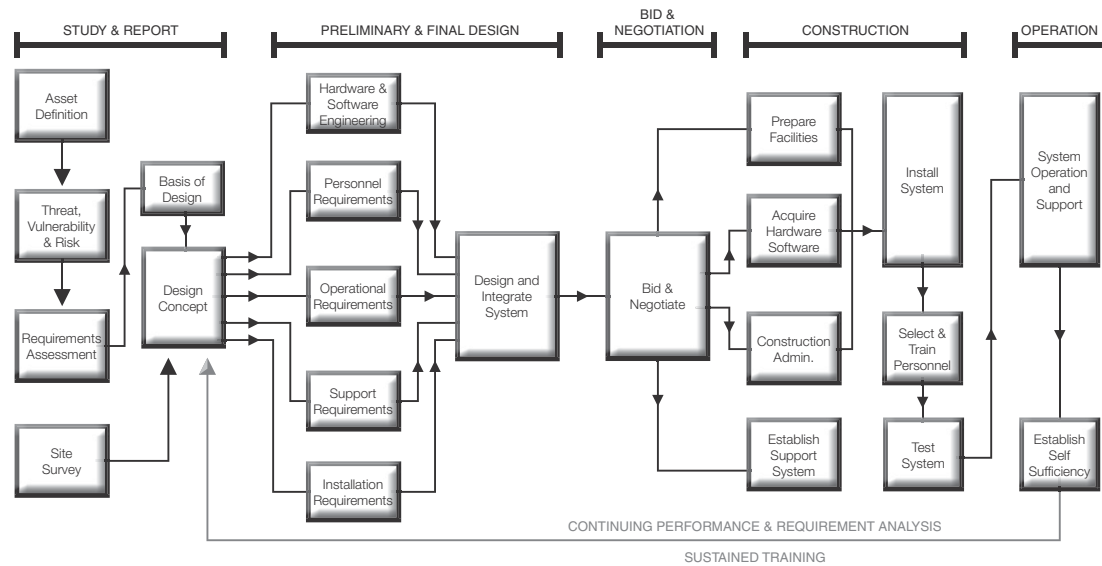


Figure 12-1
Systems Design Process

In simpler form, the process starts with the planning and assessment phase. The first task of that phase is the identification of critical assets, potential threats, subsequent vulnerabilities, likely risks, and functional requirements. For example, to deter burglary, a common method is to harden the target to deter or reduce the opportunity to commit the crime. In a broader sense, this is the time to collect information on security needs, objectives, and constraints so that risk management and control can be effected before a security event rather than after. This concept of proactivity versus reactivity in security planning is a key aspect of effective risk management and control. The second task of the planning and assessment phase is to analyze security requirements and formulate solutions or countermeasures concepts to reduce or eliminate vulnerabilities and mitigate risks. Once these concepts have been validated both operationally and in budgetary terms, the design phase can begin. The output of the design phase is systems hardware and software identification, placement, integration, and performance documentation that is sufficiently clear and complete to ensure consistent, accurate interpretation by suppliers and installers for systems procurement and implementation.

The systems design process is a serial process. Each phase and task must be performed sequentially before the next can begin—the output from one task becomes the input for the next. This is an important concept for senior management. Depending on the nature of the environment, organization, and potential risks, the process requires a significant effort to develop the basis of design and resultant design documentation and construction implementation. The process can be shortened only a little when the user arranges for a design/build relationship with a contractor versus a design, procurement, and construction relationship with an architect or owner. Generally, increasing the staff or budget cannot substantially shorten the process. Moreover, if the security systems project is part of a major facilities construction or upgrade project, security systems design and implementation will be executed and documented according to the schedules and documentation of architectural design and construction, normally managed by a certified architect as project overseer. In that case, those responsible for the security design will work directly with the architect and his or her project team to document security requirements and include them in contract documents for bid and construction.

12.3 INITIAL PHASES

The planning and assessment phase is the first phase of any security design project. This phase consists of gathering all relevant pre-design asset information and analyzing it in terms of project requirements and constraints. Planning and assessment efforts always culminate in a security “basis of design,” the first and most important output of the design process. The basis of design focuses on specific project requirements and a conceptual design solution based on those requirements. These phases are focused on defining threats, identifying assets, considering vulnerabilities via analysis, and assessing risk.

Thus, security planning, assessments, and operational audits are formal processes for identifying and analyzing the security issues and problems associated with asset protection, and of developing asset protection requirements, objectives, criteria, concepts, and methods that will be used in the eventual detailed design of the solution. The assessment or survey is effective if action is taken on the recommendations and results are measured against acceptable standards. This phase involves considerable teamwork between operational, facilities, engineering, and architectural representatives to present the proposed solution to management for approval and budgeting.

Three key ingredients in the planning phase determine its eventual success. First, a multidisciplinary and committed approach from either a single individual or project team is needed. Second, spending the necessary time and effort in the planning phase results in a more accurate and responsive design solution, reduced risks, reduced overall costs of potential losses, and increased longevity and effectiveness of the installed systems. Third, decisions made during the planning and assessment phase must be made on the basis of sound and relevant risk and asset environmental information. In essence, security design is just as dependent on collecting good data leading to informed decisions by knowledgeable people as is any other analytic process where a solution is engineered and constructed.

The outcome of the overall planning phase is a set of security requirements, or objectives, that is used as a basis of the eventual design (also called design basis). Assessment consists of surveying and analyzing the assets and protection, normally through an initial site survey and vulnerability assessment, and applying the risk assessment and design process to arrive at a conceptual solution based on derived protection requirements. Thus, the planning and assessment phase results in a conceptual design solution that categorizes vulnerabilities by their criticality and identifies the most preferred and cost-effective protection scheme to mitigate or eliminate asset risks. The initial design solution at this phase of the process is entirely based on the designer’s interpretation of functional requirements in the conceptual solution. Without these requirements, there can be no meaningful design solution and precious capital may be wasted in expensive construction.

Another important outcome of the planning phase is the development of the business case for the new or upgraded security systems. Systems will be evaluated not only on quality and reliability but also on cost. The business case documents the impact of the design solution on the business, the necessary investments, expected quantifiable savings, and other metrics that allow decision makers to make investment decisions on a security project. The main feature of a security business case is a series of economic metrics (return on investment, payback, net present value of cash flow, etc.) that are used to justify the security solution up the management chain. A formal presentation on the security needs, business case, costs and benefits, alternatives, and impact on operations is often mandatory before the expenditure of capital. In the architectural and engineering world, the planning phase is typically referred to as the programming and schematic design phase leading to a design basis (requirements analysis) and conceptual design.

A requirements analysis is necessary for effective planning. Requirements analysis uses the threat, assets, and risk analysis as its basis.

Defining design requirements is the process of developing specific functional design guidance leading to security strategies. Before looking at specific asset protection requirements, it is useful to formulate a statement of the overall objectives or mission of the integrated security system (ISS). The objectives must reflect and support the overall corporate mission if the ISS is to be funded and supported by management. The overall protection objectives should be validated as each design planning task is completed. New insights will come as the process develops. It may become necessary to revise the mission statement, but at the end of the task the requirements definitions should accurately reflect the overall asset protection objectives.

It is useful to add a level-of-confidence factor to each functional security requirement. Thus, the terms *detect* and *delay* rather than *prevent* are useful. A security system built on absolute objectives, such as total denial of unauthorized entry (100 percent confidence), will either be impossible to design or so costly as to be impractical. The real danger is not unauthorized entry itself but the consequences of such entry. The requirements definition should focus on preventing, delaying, or modifying the consequences.

Design solutions to various asset vulnerabilities may be the same, similar, or complementary. For example, a security requirement that leads to the detection and delay of unauthorized access may be partially or completely applicable to another perceived asset vulnerability, such as the prevention and deterrence of trade secret theft by a business competitor. A thorough planning process must evaluate all asset vulnerabilities and list specific functional requirements and resultant protection strategies.

The level of protection for a group of assets must meet the protection needs of the most critical asset in the group. However, the designer of a security system may separate a critical asset for specific protection instead of protecting the entire group at that higher level. Thus, the requirements analysis and definition process is designed to do the following:

- Ensure that the selected solutions will mitigate real and specific vulnerabilities.
- Provide a cost/benefit justification for each solution.
- Identify all elements (technology, staffing, and procedures) and resources required for each solution.
- Provide a basis for the accurate and complete system specification that will be used to procure and implement the solutions.

Figure 12-2 provides an example of a requirements analysis completed for a specific project.

| | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| The entrance to the building is at the first floor and is flanked by a real estate office and a bank. There are two entrances, a north entrance and a south entrance. There is an exit door at the east side of the building. The real estate office and bank have staff members and visitors accessing their facilities. There must therefore be a demarcation of facilities on entry to the building. Security is essential at this level as the elevator lobby and day care center are susceptible to entry by visitors other than those coming to visit. | | |
| | First Floor | |
| | Door 1 | Door 2 |
| Use | Access to terrace from within the office | Secondary door to day care facility |
| Assets | HR office Personnel files | Day care center equipment Children's records Children |
| Criticality | Medium | Medium |
| Threats | Break-in Arson Theft of records Theft of equipment Door left open | Break-in Theft of records Theft of equipment Door left open Child abduction |
| Vulnerabilities | Fire engulfing whole floor HR info being compromised | Compromise of safety and care at day care center |
| Risk | Injury to personnel Loss of records Disruption to work processes Psychological danger | Injury to personnel and children Loss of records Disruption to work Psychological danger |

Figure 12-2
Requirements Analysis

12.3.1 BASIS OF DESIGN

Once the requirements definition is complete and the individual design requirements are identified, the designer prepares a basis of design and submits it to the design team. The basis of design documents the initial designation of assets deemed critical, outlines the overall objectives of the asset protection program, describes the results of the risk analysis, lists the functional requirements to be satisfied by the eventual design, and provides a narrative operational description of the proposed systems, personnel, and procedures that constitute the security system or program.

The basis of design becomes the designer's means to obtain consensus from the design team on the goals and objectives of the project, what will constitute the project, and how the project will secure the assets. Each member of the design team should have input into the design basis. This is not the time to identify engineering details, prepare budgets, or identify and debate specific countermeasures. This is the time when the project is first conceived, the requirements are derived from a rigorous risk assessment, and subsystem functional descriptions are provided to indicate eventual system performance. Also, this is the time when initial site surveys may be accomplished to gather information on existing conditions and measures and on any needs for upgrades or additions.

12.3.2 CONCEPTUAL DESIGN

The conceptual design, also called a design concept, is the last task of the planning and assessment process and is initially developed as a product of the VA. In this task, the designer formulates a complete security solution for the assets to be protected. The security solution typically consists of protection strategies grouped together to form an asset protection program or augment an existing one. Thus, the solution normally includes security systems complemented by procedures and personnel. At the conceptual stage, however, the solution is expressed in general narrative and descriptive terms accompanied by an initial budgetary estimate for design and construction.

The design concept incorporates the basis of design; documents the findings, conclusions, and recommendations from any initial surveys; and is the first opportunity to document the project's design. From an architectural perspective, the design concept is usually referred to as the initial conceptual design or schematic phase.

The security designer collaborates with the site owner on an integrated, holistic approach to asset protection. The designer is principally concerned with establishing protective measures generally configured in concentric rings around protected assets to make it progressively more difficult for an intruder to reach critical targets and escape undetected. These protection-in-depth or redundant schemes build barriers or time delays into the intruder's path to protected assets and make it possible for other security resources to respond.

The importance of having a redundant security system is based on the 10 principles of probability developed by the French mathematician and astronomer Marquis de Laplace (1749-1827). According to Laplace's formula, when events are independent of each other, the probability of their simultaneous occurrence is the product of their separate probabilities. Thus the probability that one detection system in the security system might be circumvented is high, but the probability that all the detectors and barriers in an in-depth or redundant security scheme would be compromised is very low.

There is some debate as to the level of detail to include in a design concept. Normally, the concept includes the elements noted above, plus some initial design detail. A design concept's detail should never be more than a top-level description of the various anticipated security system elements, subsystems, and support systems.

The intended subsystems should be narratively described in the concept, as should their interaction with one another to form a complete system. The narrative details should be accompanied by representative details on specific, anticipated design aspects, such as an access-controlled entry door, an emergency exit, etc. Finally, overall block diagrams should be prepared depicting systems, subsystems, and representative element-level connectivity accompanied by project construction cost estimates.

For architectural purposes, it is common to mark up architectural floor plans with intended devices, control points, and system connectivity to give the project planners an indication of the scope and depth of interface (power, etc.) for the security portion of the project. Architects thrive on detail and take every opportunity to demand that that level of detail be included early in their project leaving.

At some point, the project must be approved. The concept level is the ideal time to seek management approval since the project team has reached consensus on the project's scope and sufficient detail has been developed to create an initial budget.

The designer's choice of countermeasures depends largely on their cost-effectiveness. Cost-effectiveness criteria that might be used include operational restrictions, nuisance alarm susceptibility, installation cost, maintenance costs, probability of detection, mean-time-between-failure, contribution to manpower reduction, contribution to asset vulnerability, and reduced risk, normally expressed in the monetary consequence of loss or destruction.

A designer may choose from many countermeasure options. Most security designers identify four principal security strategies—prevention, detection, control, and intervention—as the most important functional requirements of security design. Homeland security features five principal strategies: preparation, prevention, detection, response, and recovery. Figure 12-3 shows a sample countermeasures development table.

| Floor | Door | Use | Assets | Criticality | Countermeasures |
|----------|-------|----------------------------|-----------------------------|-------------|-----------------------------------|
| Basement | 1 | Loading dock | Incoming materials | Medium | Surveillance Access control |
| | 2 | Shipping/receiving/storage | Stocks/products | Medium | Access control |
| | 3 & 4 | Door leading into corridor | General equipment | Low | Intercom Access control |
| | 5&6 | Shipping/receiving office | General equipment Stocks | Medium | Duress Door release Monitor |

Figure 12-3
Countermeasures Development Table

12.4 DESIGN CRITERIA

Design criteria constitute the ground rules and guidelines for the design. In effect, these are additional design requirements that the design must consider along with risks. The criteria fall into a number of categories, some based on expected system performance, some on operational and financial considerations, and others on style, design, codes, and standards. Not all asset protection measures are possible or practical. Other criteria will identify constraints or limitations that apply to the design, implementation, and operation of the system.

At this phase of the design process, it might only be necessary to list the criteria rather than include a complete description of the details. The details will be included in the design specifications and construction or contract documents. Some of the more influential design criteria are described below.

12.4.1 CODES AND STANDARDS

Particularly for facility security design and upgrade projects, design and implementation will probably have to follow national and local building, fire, and life safety codes. Applicable codes must be identified and applied to the initial design to ensure compliance. In addition, various laws may come into play, including those regarding security officer registration and training. Also, the organization may have its own set of standards for design, procurement, modification, and construction, such as work rules, insurance coverage, acceptable color

schemes, and competitive bidding rules. Some organizations even have a set of security standards or guidelines that establish design and construction standards for security system implementation. Certain life safety codes have a significant effect on the selection, configuration, and operation of components selected to control doors. Failure to adhere to these codes and standards may lead to eventual rejection of the design solution in the construction phase, and meeting codes may require expensive changes to the constructed system. This occurs particularly where security controls are applied at junctures in the building's established path and it is later determined that such controls violate the safety code and must be eliminated. Other cases involve the use of particular locking mechanisms (such as electric strike, electromagnetic, and vertical pin locks), their application to certain door types, and the resultant door hardware configuration necessary to meet codes.

12.4.2 QUALITY

A designer should always be aware of the quality and performance differences between components. Generally, the use of quality components in a superior design goes a long way. A good design always strikes a balance between quality components and overall cost. Quality also needs to be applied consistently. For example, it makes little sense to install a high-quality lock in a hollow wooden door, a metal door surrounded by simple drywall construction, or an intrusion alarm system with sensors and a control unit but without an alarm communication and display system. The alarm system must also have tamper protection that provides an alarm signal if the system is compromised. The designer always identifies options to make it easier for management to understand cost drivers and the relative performance of different configurations. It is also important to document the trade-offs between cost and quality.

12.4.3 CAPACITY

Capacity, size, and space requirements are major determinants of security system solutions. Desired capacity (for example, number of card holders for an access control system, number of alarm zones monitored, number of access controlled doors, etc.) may be changed as the design is developed. Still, having a general estimate at this stage reduces the number of design iterations. Nothing complicates a design more than a restatement of system capacity requirements midway through the design process. The designer always considers expansion capacity in the design from the very beginning, typically adding anywhere from 10 to 15 percent spare capacity.

12.4.4 PERFORMANCE

Component performance is usually detailed in a performance or project specification. Overall system performance parameters, however, should be stated as design criteria in the design basis documentation as well, especially if the designer intends for systems to interact with existing systems or conditions. The following are examples of performance parameters:

- The entry control system must connect to an existing local area network.
- The entry control system must effectively manage personnel traffic at shift changes.
- The card reader-controlled turnstile subsystem must have a minimum throughput of 500 badge holders per hour and be able to accommodate building evacuation within 10 minutes.

The performance list can also include reliability and maintainability criteria—for example, that the turnstile must have a mean time between failure (MTBF) of 2,000 hours.

12.4.5 FEATURES

Major system features should be summarily defined in the basis of design documentation and eventually in more detailed terms in the performance specification. A good example is the placement of optical turnstiles in the lobby of a high-rise building, based on throughput and evacuation requirements. The throughput feature usually dictates the number of lanes, and most lobbies can accommodate only so many lanes. If the design basis requires functions that include design features that are not commonly available, procurement competition will be limited and costs could escalate. Custom features may also complicate component interface, require additional procurement and implementation time, and be more difficult to maintain. Designers should have a detailed knowledge of performance features that are normally available off the shelf. It is worthwhile to perform a reality check of both systems performance and feature design criteria with several manufacturers before finalizing the list.

12.4.6 COST

Two of the main cost drivers for security design are the design fees and projected system construction costs. Regarding design costs, some owners elicit the assistance of installer/integrators to design systems, thereby saving design costs. Others prefer to seek professional assistance from a knowledgeable consulting engineer. Over the long haul, it is beneficial to have a knowledgeable person lead the integrated design process. That person's expertise can help reduce costs of construction, personnel, and procedures. Some people experience shock when they see how expensive reasonable security can be, particularly integrated

security systems involving entry control, intrusion detection, and CCTV. If the risk analysis has been thoroughly documented and is quantitatively based, then additional funding may be easier to justify. A budget is often a required design goal and should be included as one of the initial design criteria.

12.4.7 OPERATIONS

Two main criteria drive security designs. First, security programs need to have minimum negative impact on productivity and facility operations. Restricted access in production areas may affect operations, especially if those areas experience high volumes of traffic. Hence, operations managers should be consulted early in the process to find alternate solutions (such as a new layout for a production area). Second, security operations should be seen as a natural use of security systems. For example, a systems design should include the capability to adjust to both shift changes and normal patrol operations. A good system design allows for timing of system activations while also providing for a central location where alarms, video surveillance and assessment, and communications can be monitored.

12.4.8 CULTURE AND IMAGE

Corporate culture is a significant factor in the design and implementation of security systems and programs. Culture is what distinguishes one organization from another, and it determines how security is defined and implemented in a particular organization. Care must be taken to ensure that procedures and training maximize people's acceptance of change. Related to culture is image, the perception of the organization by the outside world. Several factors, such as customer service, promotional activities, and exterior and interior facility design, help to form an image. If the security function is to support corporate goals, the security program must reflect the corporate image. Whether the program emphasizes high-profile or low-profile security, it should always consider the aesthetics of visible security components, such as security officer uniforms and security equipment. Some of these design topics may be covered by the corporate standards discussed earlier; criteria not covered above should be listed here.

12.4.9 MONITORING AND RESPONSE

An essential component in any security system and program is the design of a centrally located security operations center and the assignment of security staff to monitor alarm systems and respond to alarm conditions. The design of a central monitoring facility is becoming more important as the need for business continuity increases. In addition, as more organizations apply integrated security systems on a global basis, effective and efficient monitoring and response may become even more important. If the budget

restricts the design of a security operations center or the availability of suitable staff, the system design will need to minimize monitoring requirements or personnel or incorporate the capability for outside monitoring. For enterprise systems, a third-party monitoring and response arrangement calls into question the investment in an enterprise system in the first place. However, for some remote or single locations, intrusion detection and entry control alarms may report to a commercial central alarm station or be annunciated and controlled through a proprietary, on-site system. CCTV systems can also be applied on an enterprise basis. Such systems can be remotely monitored and used as assessment tools for local alarms, and they can also be used as archival mechanisms to retrieve previous alarm or transaction scenes at selected points across the enterprise network. The monitoring and response function used in rudimentary systems for small or medium-sized facilities can be provided by a central station. For more complex systems and larger organizations, the preferred method of monitoring and response is by on-site security staff in a properly designed and outfitted security operations center. In some cases, organizations choose to use on-site staff during the business day and remote monitoring after hours. For on-site functions, the skills and training of staff should match the complexity of the monitoring, control, and response systems.

12.4.10 PRELIMINARY COST ESTIMATE

An additional product of the planning phase is the initial budget, both for capital expenditures and recurring costs associated with the proposed system. Since at this early phase no detailed design work has been performed, nor have component quantities been finalized, the budget can be a conceptual, order-of-magnitude estimate at best. Some designers with experience in estimating the systems to be implemented can estimate within 10 percent of final bid prices. Most people, however, need assistance from vendors, manufacturers, or contractors to obtain MSRP (manufacturer's suggested retail price) for the equipment, installation, software, and support systems. The services of a knowledgeable, independent security consultant may be required.

One danger of an inadequate initial budget is that the designer may have to repeat a lengthy, difficult budget approval process. If a specific hardware vendor will supply most of the equipment desired, that vendor's expertise can be helpful in developing an initial estimate. Although that estimate is conceptual, its accuracy is important. Generally, it should be within 15 to 20 percent of final bid prices. If it is too low, later discovery of the real cost of the project could lead to its cancellation or insufficient funding to construct a totally responsive security system. If the cost estimate is too high, the initial budget may not be justifiable and may not be approved.

The following are examples of items that should be considered in the estimate:

- Capital projects
 - all equipment and support systems and their installation cost, including all primary and backup systems, software, components, mounting hardware, sensors, termination panels, control panels, back boxes, junction boxes, conduit, cable, battery backup power, uninterruptible power supplies, and main power circuits
 - freight, taxes, etc.
 - project management and supervision labor
 - shop drawing submissions
 - testing
 - commissioning
 - operator and user training
 - as-built (record) drawings
 - warranty
 - design fees
- Service projects and recurring costs
 - security staff payroll, including supervision, benefits, holidays, vacations, and sick leave
 - uniforms and equipment
 - training
 - equipment maintenance, repair, and replacement
 - consumable supplies, including printer paper, ink and toner cartridges, and backup media
 - replacement access control cards, badges, and review of development procedures
 - central alarm station monitoring and response

For early phases of the project, the estimate would provide a single, lump-sum estimate for each subsystem and the total systems, often in a simple narrative format. Later budgetary estimates are more detailed, like the one in Figure 12-4.

| FACILITY SECURITY SYSTEM COST ESTIMATE | | | | | | | | | | |
|-----------------------------------------------|--------------|---------------|------------|----------|------------|-------------------|-------------|------------|-----------------|-----------------|
| Head End | Manufacturer | Model | Unit Cost | Quantity | Base Price | Installation Time | Hours Labor | Labor Cost | Installed Cost | |
| PC Workstations (Computer/Monitor/Keyboard) | Dell | Optiplex GX1p | \$2,800.00 | | \$0.00 | 4 | 0 | \$0.00 | \$0.00 | |
| Application Software – Network | WSE | NSM | \$7,500.00 | | \$0.00 | 8 | 0 | \$0.00 | \$0.00 | |
| Alarm/Access Printer | Epson | 570-PRT | \$600.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Network Hub | Lancast | 4490 | \$285.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| | | | | | | | | | | \$0.00 |
| Access Control | | | | | | | | | | |
| Access Control Panel | WSE | 4100 | \$2,445.00 | | \$0.00 | 6 | 0 | \$0.00 | \$0.00 | |
| Alarm Input/Output Board | WSE | MIRO 16/8 | \$1,090.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Signal Multiplexer | WSE | Nexstar | \$300.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Enclosure (30" x 36") | WSE | 92410080000 | \$250.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Panel Power Supply | Alarm Saf | PS-1 | \$500.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Lock Power Supply | Alarm Saf | PS-5 | \$280.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Proximity Cards – Thin | WSE | QuadraKey | \$5.00 | | \$0.00 | 0 | 0 | \$0.00 | \$0.00 | |
| Card Reader – Proximity (Surface Mount) | WSE | DR4205 | \$480.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Network Connection | | | \$195.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Modem/Telephone Connection | | | \$195.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Terminal Server | WSE | Cobox E2 | \$545.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| | | | | | | | | | | \$0.00 |
| Photo ID Equipment | | | | | | | | | | |
| Photo Identification System PC | Dell | Optiplex GX1p | \$2,800.00 | | \$0.00 | 4 | 0 | \$0.00 | \$0.00 | |
| Photo Identification System Software | WSE | QuikWorks 4 | \$4,250.00 | | \$0.00 | 2 | 0 | \$0.00 | \$0.00 | |
| Photo Identification System Camera | Kodak | DC210 | \$900.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Photo Identification System Frame Grabber | WSE | Image Capture | \$600.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| Photo Identification System Printer/Laminator | Fargo | Pro-L | \$7,440.00 | | \$0.00 | 1 | 0 | \$0.00 | \$0.00 | |
| | | | | | | | | | | \$0.00 |
| Hourly Labor Rate | | | \$65.00 | | | | | | | |
| Total Parts and Labor | | | | | | | | | \$0.00 | \$0.00 |
| Estimated Sales Tax | | | | | | | | | \$0.00 | \$0.00 |
| Estimated Freight | | | | | | | | | \$0.00 | \$0.00 |
| Estimated Permits | | | | | | | | | \$250.00 | \$250.00 |
| TOTAL ESTIMATED COST | | | | | | | | | \$250.00 | \$250.00 |

Figure 12-4
Sample Cost Estimate Format (Circa 2007)

A more detailed discussion is presented in Appendix A: Estimation.

12.5 DESIGN TEAM

Security design does not exist in a vacuum. Security managers and directors need to determine who in their organizations should be involved in the design process and what their relationship should be with the design and construction professionals. The players should be identified early in the planning process—as soon as the extent of the project is known—so they can contribute to the initial preliminary design process and benefit from knowledge of it. The management style of the organization will determine the selection of those team members, as will the site and nature of the project. Not all those in the following list will necessarily be included in the team. For example, the design team roles of the CEO and CFO may be performed by their delegates. The following are possible members of the design team:

- **Chief executive officer.** The CEO is involved in the project for two major reasons. The first is to ensure that the goals of the security program reflect the corporate mission and that the corporate image is maintained or enhanced. The second is to provide top-down support for the security program. Nothing can scuttle a well-designed program more quickly than lack of interest by executive management.
- **Chief financial officer.** The CFO keeps an eye on the cost/benefit factor of the project and approves funding once it is justified. The CFO is accustomed to reviewing quantitative data and bases investment decisions on returns.
- **Human resources manager.** Some security procedures are managed by the human resources department, such as careful hiring and firing practices and maintenance of an access control system cardholder database. Also, in many organizations the security function reports to the human resources manager.
- **Information technology manager.** Information technology is both an asset and a vulnerability. Particularly where security systems operate on an enterprise network, the information technology department should be involved to ensure that corporate standards are maintained.
- **Facilities manager.** In larger organizations, facilities management is closely aligned to the security function, especially regarding security technology and systems monitoring.
- **Project architect.** For projects involving major construction, an architect is usually involved.
- **Construction manager.** Larger construction projects may include a specialist firm that is responsible for all construction and implementation. The construction manager usually gets involved early in the design process to keep an eye open for constructability, design approval, and cost issues.
- **Security system designer.** Security subsystems and their integration are becoming increasingly complex, so considerable experience is required to design a system that addresses both vulnerabilities and operational issues. In larger organizations this capability may be available in-house. However, since new system projects do not occur often within an organization, it may be useful to retain a consultant who has relevant experience and no vested interest in any service or equipment being provided.
- **Security manager.** The security manager's role is essential to the successful design and implementation of the system. The security manager should understand these important concepts:
 - The system does not belong to the architect, security consultant, system vendor, users, or even CEO or shareholders. The security manager lives with the consequences of system failure and therefore must assume accountability and ownership of the system. Ownership is achieved by understanding the process of design and implementation and by maintaining direct involvement throughout the project.

- One person cannot master all aspects of design and construction. Security managers who resist hiring specialists may end up relying on the inadequate expertise of company employees or security vendors. The security manager should identify where expertise is lacking and be prepared to hire specialists—as employees or consultants—to help him or her maintain the level of involvement required to achieve ownership.
- To be successful, the system solutions must reflect the organization's mission, must be responsive to the organization's culture and business operations, and must have executive management's approval and involvement. For these reasons, the project team should prepare a security business case using terms and approaches common to other corporate capital investment projects.

12.6 DESIGN AND DOCUMENTATION PHASE

Next the project moves into the design and documentation phase. In the construction design industry, this may be split into two phases, the design development phase and construction documents phase. Alternatively, it may be considered a single phase called construction documents, or CDs, with the completion of the design development work being referred to as 30, 35, or 50 percent. Generally, design development includes a preliminary design (30 to 35 percent) following the conceptual or schematic design and concludes with a 50 to 60 percent design development. The percentages represent the level of completion of the final construction documents.

Following design development, CDs usually begin with a 60 percent design and pass through a 90 percent CD phase submission to conclude with a 100 percent CD set. If the security designer is working with an architect, design phases and submissions usually coincide with those reflected in the contract between the architect and the owner. However, if the security designer is working without an architect, these design submissions are usually tailored to the specific project and almost always include a conceptual, preliminary, and construction set submission with corresponding design reviews at each phase.

The objective of the design and documentation phase is to complete the design and to document the process to the level of detail necessary for the chosen method of procurement. A greater level of detail in the design will lead to better responses from bidders and lower project costs.

The complete set of procurement documents, known as contract (or bid) documents, will consist of three sections: contractual details, construction specifications, and construction

drawings. In a procurement of services (such as security officer services), the third section is not required. In a construction-related procurement (involving, for example, access control and CCTV), the specifications and drawings are called construction documents. On smaller projects, it is common to see all the written specifications included on the construction drawings.

12.6.1 CONTRACTUAL DETAILS

This section of the contract documents describes the form of contract to be used when a supplier has been chosen. It covers insurance and bonding requirements, site regulations, labor rules (union or non-union, wage rates, etc.), delivery and payment terms, methods of measuring work progress for partial payment, owner recourse in the event of nonperformance, termination conditions, application of unit pricing to additions and deletions, instructions to bidders, etc. For a large construction project, the architect or the owner's construction manager develops this document to cover all trades, including security. For smaller jobs, the company's purchasing department may develop this section. In most cases, the document is included in the contract documents and is modified to suit the particular project as the project progresses.

12.6.2 SPECIFICATIONS

The systems specifications mirror and complement the actual systems design in sufficient detail to achieve the following:

- The final implementation reflects what was intended. In all cases, the systems specification contains the actual performance instructions and criteria for constructing the systems included in the design. Included in the specification should be functional testing to ensure the system will do what it is designed to do as well as a continual periodic programmed testing to ensure the integrity of the system over time. Drawings and plans are virtually useless and are open to interpretation unless there are associated specifications detailing construction and systems performance criteria. Drawings and plans show what is to be constructed, whereas the specification details the owner's intent and how it is to be constructed.
- All bidders get the same, complete understanding of the requirements. Incomplete or inaccurate specifications can lead to wildly different bids and an inability of the procurer to compare them.

Because of the level of detail required, specifications tend to be wordy and very technical. Considerable technical experience in the design, procurement, construction, and operation of a security system is needed to prepare good specifications. With poor specifications,

vendors may make quality and performance choices for the owner without the owner's knowledge until the system is installed and operating.

Boilerplate specifications are available as a starting point for customization to meet project-specific requirements. Most experienced security system designers have developed their own master specifications. The specification should reflect lessons learned from previous security system projects. For example, a contractor may have misinterpreted a phrase in the specifications, leading to reduced functionality of the system or increased costs.

Specification sections are numbered depending on the construction trade so that each section can be issued separately. Standard specifications are available from the American Institute of Architects (www.aia.org) and the Construction Specifications Institute (www.csinet.org). For example, the Construction Specifications Institute publishes MasterFormat™ and MasterSpec™ standards. A project manager or architect would use the various divisions of those standards to document an entire construction project. Electronic Safety and Security is Division 28 of the Facility Services Subgroup.

Especially with the trend toward integration among subsystems and procurement of all security systems through a single contractor, it is common to depart from this format and include all the security systems within a single, custom-designed section. Most architects and project managers prefer the security systems all in one specification.

Each individual specification section consists of a standard format divided into three parts: general, products, and execution. Each part is divided into subsections and sub-subsections. Not all titles are applicable to every project, so the specification format is often modified by the security designer to suit the unique circumstances of the project. The importance of the standard format is to ensure the following:

- The final specifications are complete in all details.
- Contractors can easily find specific details when preparing a proposal or bid or when implementing the system.

A security system specification should include the following, at least:

- **instructions to bidders** with a list of all documents included in the contract documents
- **list of project references**
- **functional description** of the complete systems design, its intended functional operation in a concept of operations, maintenance and warranty requirements, quality assurance provisions, and installation schedule
- **list of design drawings**

- **list and description of products and services to be included in the contract**
- **list of required products and services included in other contracts** (such as electrical door hardware, which is provided and installed under the door hardware contract but must be connected to the security system by the security contractor)
- **list of applicable codes and standards**
- **support services**, such as drawing, sample and documentation submittals, commissioning, testing, training, warranty, maintenance, and spare parts
- **technical descriptions** of all major subsystems and their components, including capacity, capability, expandability, performance and operational parameters, environmental operating parameters, installation and integration details, appearance and finish, and acceptable makes and models
- **general site conditions**, installation standards and quality control standards

Appendix B: Implementation shows a model specification for reference.

12.6.3 **DRAWINGS**

Along with specifications, drawings are the cornerstone of any construction project. A picture or diagram of design intent is less likely to be misinterpreted by contractors. However, to avoid ambiguity and to manage any discrepancies among the drawings, specifications have precedence over drawings.

Most drawings are produced by computer-aided design drafting (CADD) systems. Compared to manual drawings, CADD files are clearer, modifications are quicker and less expensive to make, and documents can be shared more easily. In addition, many security designers themselves work directly with CADD systems rather than making sketches for a draftsman to convert into a finished drawing. The direct approach eliminates transcription errors and the need to train an additional person on project engineering requirements.

Security system drawings usually consist of plans, elevations, details, risers, and hardware schedules. Each drawing is either a site plan or floor plan showing the security systems devices by type and location. The floor plan in Figure 12-5 is one such drawing.

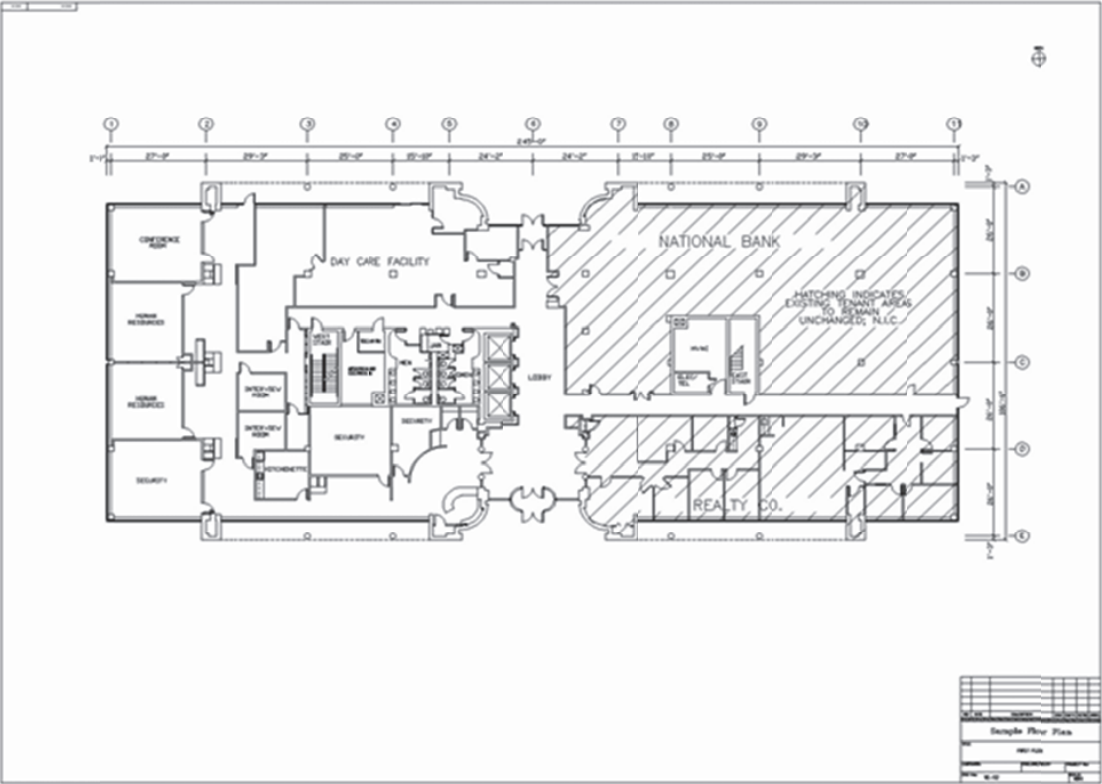


Figure 12-5
Typical Floor Plan

Plans

Each security systems plan shows a top-down, map-like view of an area where security devices and systems are located. The area may be a complete site, a building floor, or part of a floor. Many plan drawing sheets as needed to show all areas where security systems will be installed. The background information on a plan drawing consists of such items as fence lines, building wall locations, interior partitions, doors, furniture, door and room numbers (known as targets or tags), room names, floor materials, stairs, fixed equipment, etc. The architect usually provides the background drawings for a construction project. For a system upgrade project, the company may already have background drawings. For manual drafting, the background information is provided on transparent (also known as reproducible) sheets, such as paper vellum or Mylar, onto which are drawn the symbols that represent the various items of security equipment and, in some cases, lines between equipment to show interconnections. The level of background detail must be sufficient but not so extensive that the drawings become busy and security equipment becomes inconspicuous.

The background drawing file consists of a number of layers (for example, one each for walls, doors, furniture, and lighting design). The CADD draftsman can select which levels are required and turn them on or off. Security symbols are usually kept on their own layer and are copied to required locations as predefined blocks. If the architect changes the background design, the old security layer can be superimposed on the new architectural background. Changes to the security layer only need to be made when security is affected by the architectural change, such as new or relocated alarm doors.

Many individual companies, security magazines, architects, engineers, security consultants, and standards-making organizations have developed sets of security symbols. The most common symbols set for manual drafting is issued by the ASTM International in *Standard Practice for Security Engineering Symbols*, (2011). In 1995 a standard for symbols was developed jointly by the International Association of Professional Security Consultants and the Security Industry Association. Titled *Architectural Graphics Standard—CAD Symbols for Security System Layout*, the standard provided symbols that were incorporated into the ASTM standard. Whichever set of security symbols is used, the specifications should require that the same set be used for contractor-submitted drawings. Figure 12-6 presents a drawing detail showing symbology to depict security devices. It also depicts a numbering scheme for security devices for later reference in schedules.

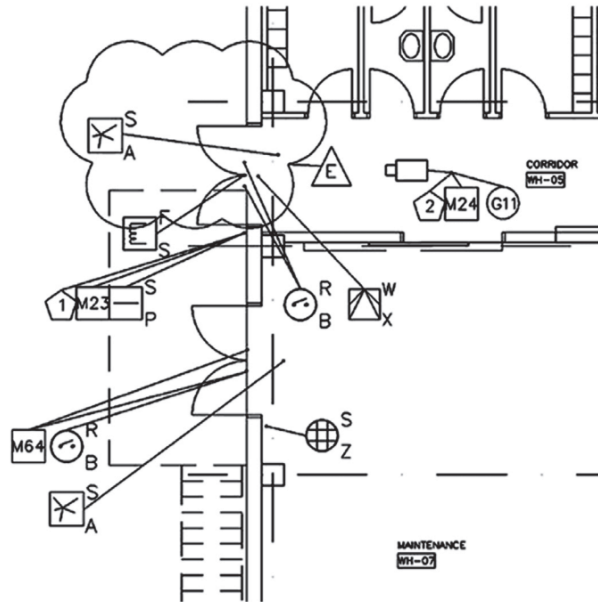


Figure 12-6
Typical Drawing Device Symbology

Elevations

Elevations are views of vertical surfaces and are included to show mounting heights and locations of wall-mounted devices, such as cameras, card readers, and motion sensors. Elevation backgrounds can be provided by the architect or from the organization's files. A sample security door elevation is shown in Figure 12-7.

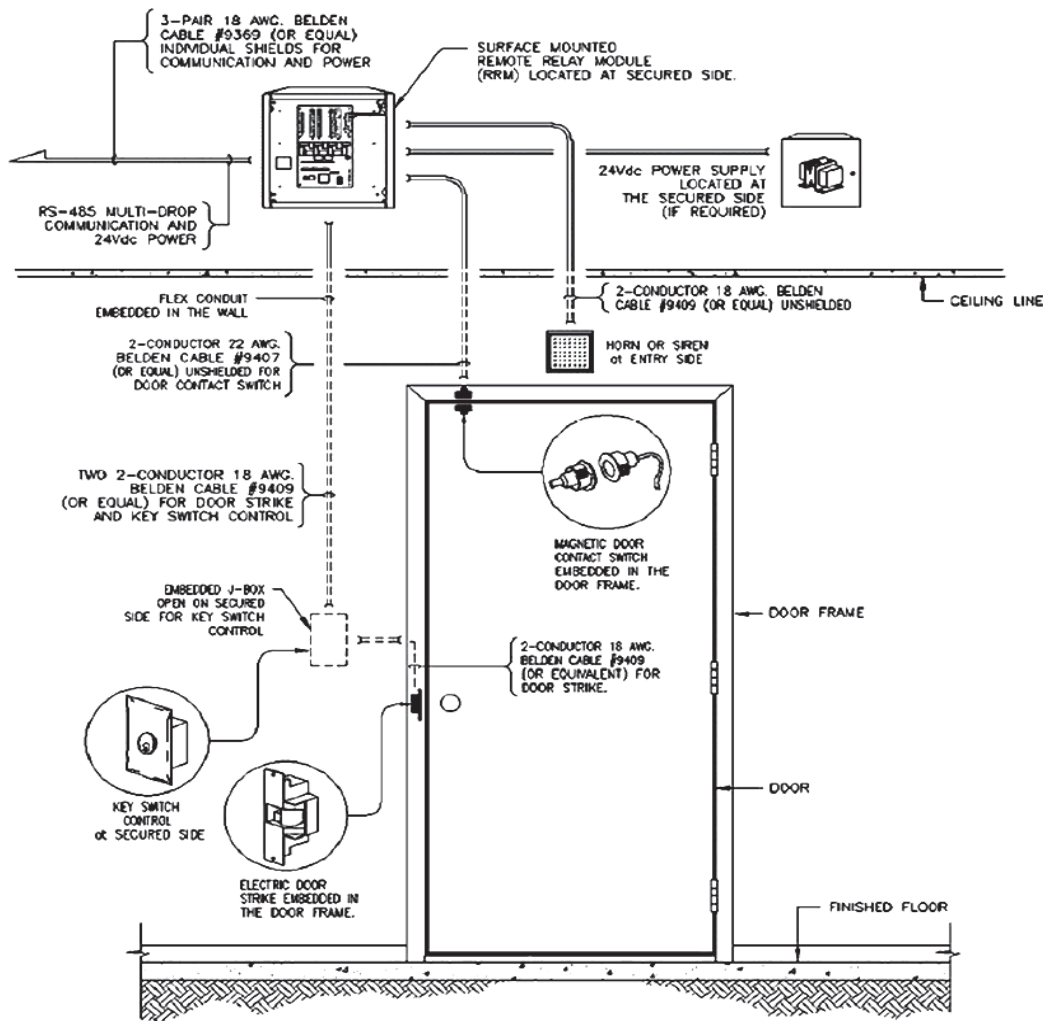


Figure 12-7
Security Door Elevation

Details

Most plans and elevations are shown in small scale for the drawings (for example, 1/8 inch equaling 1 foot). Detailed drawing sheets can be developed to define elements of the system in more detail. Such details may include special mounting techniques, custom part design dimensions, or cable terminations. These are usually developed specifically for a project. However, a security system designer may have access to drawings from previous projects that can be reused or modified.

Risers

Riser diagrams are representations of complete subsystems, such as CCTV or access control. They schematically demonstrate all the associated devices and components and their interconnecting cables. For a campus environment, each building may be shown as a different block. For a high-rise building, each floor may be shown in a vertical, elevation-like format. On smaller projects, all subsystem riser diagrams, with their interconnections and interfaces, may be placed on a single sheet. Because so much information is depicted on a single drawing, it is used by designers and contractors as the master drawing. In particular, contractors tend to use the riser diagrams for device counts when developing their bid price for the project. For these reasons it is important that riser diagrams be accurate and complete. Figure 12-8 shows a sample of a small riser diagram.

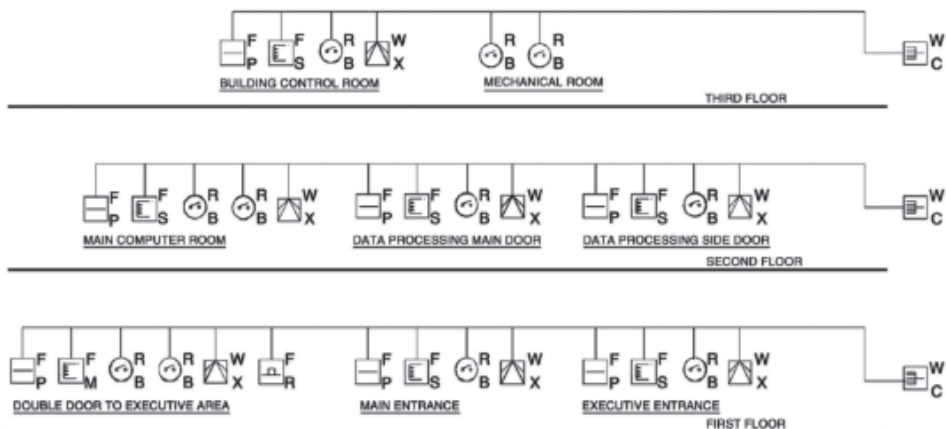


Figure 12-8
Sample Riser Diagram

Hardware Schedules

Hardware schedules are tables of related security devices. They provide detailed information that cannot easily be shown on drawings or in the text of a specification. Schedules are used for door hardware, control devices, intrusion sensors, cameras, monitors, and other devices that appear repetitively, such as termination panels. Figures 12-9 and 12-10 show sample hardware schedules for security door-related devices and CCTV cameras. The schedules are often shown on security drawings but may also be appended to security system specifications.

| # | Floor | Location/Room | Door | Access | Electric Lock | Other Hardware |
|-----|----------|----------------------------|------|-------------|---------------|--------------------------------------------|
| B01 | Basement | Loading Dock | | | | Intercom |
| B02 | Basement | Shipping/Receiving/Storage | DBL | Card reader | Strike | 2 door contact (recessed), request to exit |
| B03 | Basement | Shipping/Receiving office | SGL | Card reader | Strike | 2 door contact (recessed), request to exit |
| B04 | Basement | Shipping/Receiving office | | | | Intercom |
| B05 | Basement | Shipping/Receiving office | | | | Monitor |
| B06 | Basement | Shipping/Receiving office | | | | Telephone |
| B07 | Basement | Shipping/Receiving office | | | | Duress |

Figure 12-9
Sample Door Schedule

| Camera Number | Location/View | Type | Lens | Housing | Mount | Height | Alarm Call-up |
|---------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|---------------------------|-------------|---------|---------|---------------|
| B1 | Loading dock and area leading into the shipping/receiving area | PTZ | 10:01 | Enviro DOME | Wall | 12 feet | |
| C01 | Ground floor lobby. The field of view of this camera includes the lobby and the corridor leading to the east exit. | PTZ | 3.2 mm - 6.4 mm varifocal | DOME | Ceiling | Ceiling | Yes |
| C02 | Third floor lobby. The field of view of this camera includes the lobby. | Fixed dome (Sensormatic AD614LSP or equivalent) | 3.2 mm - 6.4 mm varifocal | DOME | Ceiling | Ceiling | Yes |

Figure 12-10
Sample Camera Schedule

12.6.4 DESIGN COORDINATION

Security design on a construction project is affected by many other design disciplines. Careful coordination among the security system designer and other design team members is essential to avoid missing elements of the design or procuring things twice. Some elements of the security system will be procured and described in specification sections that are prepared by other design disciplines. For example, in new construction it is common for all electrical power, including that required for the security system, to be described in a single specification and procured and installed by a single electrical contractor. Listed below are the various design team members with whom the security designer is usually required to coordinate.

Architect

The architect lays out the space within a facility. Any space required by the security system, such as a console, locker rooms, riser closets, or security equipment storage rooms, must be coordinated with the architect. The earlier this occurs in the design process, the more likely the security department will get the space it needs.

The architect usually specifies door hardware. In addition, the architect ensures that appearances and finishes are consistent and that any door cut-outs required for hardware installation are performed in the factory.

Electrical Engineer

The primary coordination concern with the electrical engineer is ensuring that main electrical power is provided at all locations where security equipment requires it. Dedicated circuit amperage and electrical support requirements (such as a generator or uninterruptible power supply) need to be specified.

Similarly, it is common to include electrical back boxes, junction boxes, and conduit in the electrical section of the specifications. These are installed by the electrical contractor.

If the electrical engineer is designing a separate fire alarm system, its interface to cut power to fail-safe security door locks, as required by code, needs to be fully coordinated.

Mechanical Engineer

This coordination issue relates to heating, ventilating, and air conditioning (HVAC) requirements for security spaces. The mechanical engineer needs data on heat loads and duration of occupancy (such as a 24-hour security control room or security equipment with special environmental needs) to ensure that the required environment is provided. If conduit for security cabling is required above the finished ceiling level (and its runs are not being designed by the electrical engineer), locations need to be coordinated with HVAC ductwork.

Vertical Transportation Designer

Security equipment associated with elevators, either inside or outside the cabs, requires careful coordination. The placement and mounting of CCTV cameras in cabs is critical to their effectiveness and very dependent on cab design. The designer may be on the staff of the architect or mechanical or electrical engineer or may be a specialist consultant. Other coordination issues are the inclusions in traveling cable of the security equipment's needs, power requirements on the roof of the cab, and any interfaces required in the elevator machine rooms. Use of security equipment with escalators must also be coordinated.

12.7 CONSTRUCTION DOCUMENT REVIEW, APPROVALS, AND ISSUE

During the development of the construction documents, it is common to set certain milestones at which progress is reviewed. The milestones may be target dates or nominal percentages of completion, such as 35, 60, 75, 95, and 100 percent. Smaller projects should not require as many reviews. At each milestone, it is important to compare the state of the design with the original security requirements and design criteria to ensure that the vulnerabilities originally identified are being addressed by the security system and that the security program objectives are being met. As the design progresses, the construction cost estimate should be updated to confirm that the project remains on budget. The estimate should become more accurate as the design gets closer to finalization.

When affected parties are brought into the review, their scope should be limited to the portion of the design that affects them. Some project team members may not be familiar with construction documents and may find them difficult to understand. It is often beneficial for the security designer to provide a presentation of the security system design concepts and intended operations. Comments and requests for changes should be provided in writing, and the response, together with details of any schedule or cost implications, should also be documented. Changes made early in the design process have far less impact on cost and schedule than do those made later. Also, changes made during the design phase are less expensive to implement than those made during or after installation. Changes are inevitable, but major or frequent changes may indicate a project with an incomplete or inaccurate design.

If formal approvals are required, either at each milestone or only at completion, they should be obtained before issuing final construction documents. For major construction projects, the final documents may need to be stamped—that is, imprinted with the seal of a professional engineer (PE) or architect. For security systems design stamping, it is usually the electrical PE designer who is called on for a stamp. If the security consultant/engineer does not have a PE license, he or she should be an employee of, or work very closely with, a firm

that has employees with PE licenses. No reputable professional engineer will rubber-stamp construction documents—design liability passes to the professional who stamps the drawings. The professional engineer needs to have been involved in the design process and must perform an extensive design review (and such services are not inexpensive). Since security system design work typically relies on low-voltage electrical systems, the need to stamp security drawings is infrequent and the added expense is usually unnecessary.

The completed set of contract documents (contractual details and construction documents) may be issued to bidders by the owner organization, the security consultant, or the owner's architect or construction manager. Contractual details and specifications and equipment schedules are usually produced on letter-size paper and can be photocopied. Final drawings are usually large sheets from which blueprints are made. It takes time for reproductions to be made and issued. Some government organizations that publicly advertise projects require bidders to collect and pay for sets of construction documents.

12.8 PROCUREMENT PHASE

The three major forms of security systems procurement are sole source, request for proposal (RFP), and invitation for bid (IFB), with some variations depending on whether the buyer is a government agency or commercial firm. Each form of procurement has its benefits, but the type should be selected before or at the start of the design phase. The reason is that the type of procurement affects the level of detail required in the construction documents. If an owner already has a vendor on board, a sole source procurement is appropriate and the level of detail of the design should complement the knowledge already held by the vendor. If, however, a vendor is to be chosen competitively on a wide variety of factors, such as cost, schedule, technical ability, etc., then a request for proposal is the appropriate procurement form. The vendor will require project details sufficient to submit a responsive proposal, and the owner will require sufficient vendor details to make an appropriate selection. Invitations for bid typically require sufficiently detailed design information for the responding vendors to offer a firm fixed price to install and commission the systems specified. Since IFBs key on a vendor's price, the owner must make absolutely sure that sufficient design details and instructions are provided so as not to leave any loopholes allowing vendors to substitute inferior or inadequate equipment merely to win the job.

Some large organizations have the capability to install, commission, test, and maintain their own security systems. Although their design phase may be extensive and detailed, their procurement phase may be as simple as issuing purchase orders for hardware at prenegotiated prices to prequalified vendors.

12.8.1 SOLE SOURCE PROCUREMENT

For small projects, this may be the most appropriate method of procurement. The organization prequalifies a reputable security system contractor, works with the contractor to design the system, and negotiates the cost of equipment, installation, and service. On the positive side, the construction documents are usually simple, reducing owner design costs and saving time. On the negative side, there is a tendency to focus on hardware and technology only, leaving the equally important personnel, procedures, and facilities subsystems for others. Also, the owner may tend to skip the all-important security planning process and rely on advice from a contractor with a vested interest in selling equipment. In addition, without a competitive bidding process, the organization has no means of comparing prices. This method of procurement is recommended only where the security owner has the capability to perform the security needs analysis and has good prior knowledge of systems and prices.

12.8.2 REQUEST FOR PROPOSAL (RFP)

The RFP is almost always based on a set of detailed design and construction documents. The specifications are usually generic and performance-based. Equipment makes and models are often listed with the phrase “or approved equal.” In some cases, specific models may be mandated for compatibility or commonality with existing equipment. Overall, in the RFP process the owner typically procures a security business partner, not just a one-time security systems installer.

An RFP response may be open to any contractor or it may be limited to a list of prequalified contractors. In addition to providing a cost proposal, a proposer must submit a technical proposal that describes the firm’s understanding of the requirements and how the objectives will be met. It is common to allow responders to propose alternative solutions, called “alternates.” To sensibly compare cost proposals from different contractors, it is usually necessary to require the contractors to respond to the specified design and then, if they wish, allow them to provide alternates as additional solutions. It is not uncommon to instruct proposers that alternates must produce some definable improvement in performance and be of equal or lesser cost than the base bid. The owner then benefits from the experience of the contractor while maintaining full control over the design process. The organization may select one or more of the proposers to participate in final negotiations.

The RFP need not restrict the organization to accept the lowest bid. Instead, it aims to obtain the best value. Value may be defined by the organization to suit its needs, but it should include such factors as price, quality, experience, and schedule. If price will not be the determining factor in vendor selection, the RFP should say so.

A contractor's response to an RFP usually takes longer to prepare than responses to other types of procurement because both a technical and a cost proposal must be prepared. Three to four weeks is the typical minimum proposal preparation time for medium-size to large projects.

12.8.3 **INVITATION FOR BID (IFB)**

IFB is commonly used by government and other organizations whose procurement procedures require that projects be competitively bid and that the award be given to the lowest qualified, responsive bidder. No technical proposals or alternative solutions are sought, so the construction documents must be extremely explicit. The onus of selecting equipment makes and models, and the accuracy of the security system design, is placed solely on the design team. Bidders submit a cost proposal or bid, which may contain unit pricing and whatever price breakdown is requested. Bidders may also need to show their qualifications. The award is then made, usually without negotiation, to the lowest qualified bidder who has conformed to the bidding instructions.

The IFB requires additional time and cost in design and specification, but typically needs only one to two weeks of procurement time, depending on the size and complexity of the project. It is common to require bids to be sealed and delivered by a specific time to a specific location. At the time and place, the bids are opened (often publicly) and the apparent winner is announced. Contracts are signed when the apparent winner's proposal has been checked for completeness, accuracy, and qualifications.

12.8.4 **PROCUREMENT PROCESS**

It may be important to hold a pre-bid conference to which a representative of each contractor is invited. At that conference, the owner or the owner's consulting engineer provides a complete review of the bid documents and a walk-through of affected buildings and locations. If applicable, the conference can be held at the site where the new security system will be installed so that bidders can see the field conditions. The conference should be held approximately one week after the construction documents have been issued for bid. This gives the bidders enough time to review the documents but allows time to incorporate additional information into the proposal if necessary. All questions and answers at the conference should be recorded by a design team representative in the meeting minutes. Any questions from contractors after the conference should be asked in writing, and the answers should be transmitted to all prospective contractors. It is best to set a deadline of a week before the proposal due date, after which questions are no longer taken. A single point of contact should be nominated for all questions.

Once contractor proposals or bids have been received, they need to be checked for completeness and accuracy. The contract details may say that any inaccuracies or incompleteness in the proposal will cause it to be rejected, but most commercial organizations do not reject bids unless they show signs of incompetence or gross incompleteness. It is useful to develop a matrix with column headings representing the contractors and row headings listing the main security system features and components. The matrix helps the reviewer check that the technical proposals of each responder have addressed all aspects of the construction documents. A similar matrix can be developed to compare price proposals and any alternates.

When comparing proposal costs, the life-cycle cost of each proposed system should be calculated. The first step is to identify the specific objectives and goals that the system should perform and state the expected life of the system. In its simplest form, the life-cycle cost is the sum of the capital cost and the maintenance cost over the useful life of the system. Typically, maintenance and warranty costs equal 11 percent of the total capital systems construction cost. Calculating those figures can reveal whether the low bidder has priced the system at a low profit margin but plans to make up the difference in high charges for maintenance.

If one proposal's system costs are much lower than those of the other proposals, the low proposal should be scrutinized carefully for the following:

- mathematical errors
- quality of equipment being proposed
- experience of the contractor on projects of this size and complexity
- contractor's understanding of the project
- financial stability of the contractor

All contractors' references should be checked before an award decision is made.

Interviews with the leading contenders may be revealing. In particular, the designer should request that each contractor's project manager and site supervisor (possibly the same person) be present at the meeting. The designer should attempt to determine the following:

- Is there good chemistry with the contractor's representatives?
- Do they have the experience and power of personality to work well with the other trades on the project?
- How have they resolved problems that occurred on other projects?

It also helps to find out what other clients think about how problems were resolved.

Negotiating the final price with the short list of contractors, if permitted by the procurement regulations, should be done on the basis of value. If the contractor's profit margin is too small, quality and responsiveness will suffer. A good contractor with a realistic profit will go the extra mile to ensure that implementation problems are solved and that all parties will be able to look at the finished implementation with pride. In the end, it is beneficial for the owner and contractor to enter into a business partnership, not a one-time sale.

12.9 **INSTALLATION AND OPERATION**

At this stage, the project manager should instruct the contractor on installing all system components, including any customer-furnished equipment. The contractor must install all subsystems in accordance with the manufacturer's instructions and any pertinent installation standards. The contractor should furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system. After installation, the project manager can tune the system to the specific operations of the facility.

12.9.1 **PLANNING THE INSTALLATION**

The most important step in installing the PPS is to plan correctly. All the door hardware, card readers, sensors, panels, cameras, monitors, and console equipment should already be included in the design package and located on drawings. The installation contractor should verify the locations and note any changes needed. Together, the project manager and installation contractor should examine the installation requirements and make sure all issues and differences have been resolved before proceeding.

Next, the contractor should visit the site and verify that conditions agree with the design package. The contractor should be required to prepare a written report of all changes to the site or conditions that will affect performance of the system. Also, the contractor should be instructed not to take any corrective action without written permission from the customer.

It is also important that the contractor inspect, test, and document all existing physical protection equipment and signal lines that will be incorporated into the new system. For nonfunctioning items, the contractor should provide specification sheets or written functional requirements to support the findings and should note the estimated cost to correct any deficiencies. Also, in the report the contractor should note the scheduled date for connection to existing equipment. The contractor should not disconnect any signal lines or equipment or create any equipment downtime without prior written approval of the customer. If any device, signal, or control line fails after the contractor has commenced work

on it, the contractor should diagnose the failure and correct it. The contractor should be held responsible for repair costs due to negligence or abuse of the customer's equipment.

12.9.2 COMPONENT INSTALLATION

Details on installing PPS components can be found in a standard from the National Fire Protection Association, *NFPA 731: Standard for the Installation of Electronic Premises Security Systems* (2011). General installation considerations are given in the following sections.

Card Readers

Card readers should be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required. They should be installed in accordance with local codes, the requirements of the authority having jurisdiction (AHJ), and any other applicable local, state, or federal standards.

Electric Door Strikes or Bolts

Electric door strikes or bolts should be designed to release automatically (fail safe) or remain secure (fail secure), depending on the application, in case of power failure. They should use direct current (DC) to energize the solenoids. Electric strikes or bolts should incorporate end-of-line resistors to facilitate line supervision by the system. The following are some other installation considerations:

- **Solenoids.** The actuating solenoid for the strikes or bolts should not dissipate more than 12 watts and should operate on 12 or 24 volts DC. The inrush current should not exceed 1 ampere, and the holding current should not be greater than 500 milliamperes. The actuating solenoid should move from the fully secure to fully open positions in not more than 500 milliseconds.
- **Signal switches.** The strikes or bolts should include signal switches to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. The signal switches should report a forced entry to the system.
- **Tamper resistance.** Electric strike or bolt mechanisms should be encased in hardened guard barriers to deter forced entry.
- **Size and weight.** Electric strikes or bolts should be compatible with standard door frame preparations.
- **Mounting method.** The electric strikes or bolts should be suitable for use with single and double doors with mortise or rim hardware and should be compatible with right- or left-hand mounting.

Electromagnetic Locks

Electromagnetic locks should contain no moving parts and should depend solely on electromagnetism to secure a portal, generating at least 1,200 lb. (544 kg) of holding force. An electromagnetic lock should release automatically in case of power failure. It should interface with the local processors without external, internal, or functional alteration of the local processor. The electromagnetic lock should incorporate an end-of-line resistor to facilitate line supervision by the system. The following are some other considerations:

- **Armature.** The electromagnetic lock should contain internal circuitry to eliminate residual magnetism and inductive kickback. The actuating armature should operate on 12 or 24 volts DC and should not dissipate more than 12 watts. The holding current should be not greater than 500 milliamperes. The actuating armature should take not more than 300 milliseconds to change the status of the lock from fully secure to fully open or fully open to fully secure.
- **Tamper resistance.** The electromagnetic lock mechanism should be encased in hardened guard barriers to deter forced entry.
- **Mounting method.** The electromagnetic lock should be suitable for use with single and double doors with mortise or rim hardware and should be compatible with right- or left-hand mounting.

Bell or Alarm Box

This should be mounted on the front of the facility or a location where it will be in full view of neighbors and passersby. Such placement serves as a deterrent to many would-be burglars. The alarm should be placed high enough on the building to be out of easy reach.

Control Panels

Ideally, the control panels should be located close to the main entry and exit point. They should be positioned so that they cannot be reached without a ladder, should be close to a main electricity supply, and should not be attached to combustible material.

Passive Infrared (PIR) Detectors

Standard PIR detectors should not be mounted where they might be exposed to infrared light. Placement near windows, fires, filament lamps, and heat sources such as radiators and heaters could lead to nuisance alarms.

Door and Window Contacts

These are normally fitted to external doors and windows. However, they can be fitted to any vulnerable door or window to detect opening.

Shock Sensors

These are usually fitted to areas susceptible to forced entry, such as door or window frames. Door contacts detect the opening of a door or window but not necessarily breakage. If it seems possible that an intruder might attempt to gain access by kicking a panel out of a door or breaking a window, then shock sensors or PIR detectors may be a useful complement to door contacts.

Interconnection of Console Video Equipment

Between video equipment, the contractor should connect signal paths of 25 ft. (7.6 m) or less with RG-59/U coaxial cable; longer signal paths should use RG-11/U coaxial cable or fiber-optic cable. Cables should be as short as practicable for each signal path without causing strain at the connectors. Rack-mounted equipment on slide mounts should have cables of sufficient length to allow full extension of the slide rails from the rack. NFPA 731 provides more information on connecting equipment with “category” network cable.

Cameras

A camera needs a lens of the proper focal length to view the protected area. The contractor should do the following:

- Connect power and signal lines to the camera.
- If the camera has a fixed iris lens, set the camera to the proper f-stop to give full video level.
- Aim the camera to cover the alarm zone.
- For a fixed-mount camera installed outdoors and facing the rising or setting sun, aim the camera sufficiently below the horizon that the camera will not directly face the sun.
- Focus the lens to give a sharp picture over the entire field of view.
- Synchronize all cameras so the picture does not roll on the monitors when cameras are selected.

Chapter 7 of NFPA 731 provides details on selecting the appropriate location and lenses for cameras.

Exterior Fixed Mount

The contractor should install the camera mount as specified by the manufacturer and also do the following:

- Provide mounting hardware sized appropriately to secure the mount, camera, and housing with the maximum wind and ice loading encountered at the site.

- Provide a foundation for each camera pole as specified.
- Provide a ground rod for each camera pole, and connect the camera pole to the ground rod as specified.
- Provide electrical and signal transmission cabling to the mount location as specified.
- Connect signal lines and alternating current (AC) to mount interfaces.
- Connect a pole wiring harness to the camera.

Exterior Pan/Tilt Mount

The contractor should install pan/tilt mount, receiver/driver, and mount appurtenances as specified by the manufacturer and also do the following:

- Supply mounting hardware sized appropriately to secure the pan/tilt device, camera, and housing with the maximum wind and ice loading encountered at the site.
- Install pan/tilt control wiring as specified.
- Connect the pan/tilt device to control wiring and AC power.

Monitors

The contractor should install the monitors close to the operators' eye level or lower. The contractor should connect all signal inputs and outputs as recommended by the manufacturer, terminate video input signals, and connect the monitors to AC power.

Video Recording and Switching Equipment

The contractor should install the recording and switching equipment according to manufacturer's instructions and also do the following:

- Connect all subassemblies as specified by the manufacturer.
- Connect video signal inputs and outputs.
- Terminate video inputs as required.
- Connect alarm signal inputs and outputs.
- Connect control signal inputs and outputs for ancillary equipment or secondary control or monitoring sites as specified by the manufacturer.
- Load all software as specified and required for an operational CCTV system configured for the site requirements, including databases, operational parameters, and system, command, and application programs.
- Program the video annotation for each camera.

12.9.3 **OTHER FEATURES AND CONSIDERATIONS**

Conduit

All interior wiring—including low-voltage wiring outside the security center control monitoring console and equipment racks, cabinets, boxes, and similar enclosures—should be installed in rigid, galvanized steel conduit conforming to UL standards. Interconnection wiring between components mounted in the same rack or cabinet does not need to be installed in conduits. Minimum conduit size should be ½ inch. Connections should be tight-tapered and threaded. No threadless fittings or couplings should be used. Conduit enclosures should be cast metal or malleable iron with threaded hubs or bodies. Electric metallic tubing (EMT), armored cable, nonmetallic sheathed cables, and flexible conduit should normally not be permitted except where specifically required and approved by the customer. Data transmission media should not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring. Flexible cords or cord connections should not be used to supply power to any components of the PPS except where specifically required and approved by the customer.

Grounding

All grounding must be in accordance with *NFPA 70: National Electrical Code* (2011), articles 250 and 800. Additional grounding must meet manufacturers' requirements. All other circuits must test free of grounds. Grounding should be installed as necessary to keep ground loops, noise, and surges from adversely affecting system operation.

Enclosure Penetrations

All enclosure penetrations should be from the bottom unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures, should be sealed with an approved sealant to preclude the entry of water. The conduit riser should terminate in a hot-dipped galvanized metal cable terminator. The terminator should be filled with a sealant recommended by the cable manufacturer and in such a manner that the cable is not damaged.

Cold Galvanizing

All field welds and brazing on factory galvanized boxes, enclosures, and conduits should be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

System Startup

The contractor should not apply power to the physical protection system until the following items have been completed:

- All PPS items have been set up in accordance with manufacturers' instructions.
- A visual inspection of the PPS system has been conducted to ensure that no defective equipment has been installed and that no connections are loose.
- System wiring has been tested and verified to be connected correctly.
- All system grounding and transient protection systems have been verified as properly installed and connected.
- Power supplies to be connected to the PPS have been verified as to the voltage, phasing, and frequency.

Configuration Data

The contractor should enter all data needed to make the system operational into the PPS database. The contractor should deliver the data to the customer on suitable forms. The data should include the contractor's field surveys and other pertinent information. The completed forms should be delivered to the customer for review and approval at least 30 days before database testing.

Graphics

Where graphics are required and are to be delivered with the system, the contractor should create and install the graphics needed to make the system operational. The contractor should use data from the contract documents, field surveys, and other pertinent information to complete the graphics. Graphics should have a sufficient level of detail for the system operator to assess the alarm. The contractor should also supply hard copy, color examples (at least 8 x 10 in. or 20 x 25 cm in size) of each type of graphic to be used for the completed system. The examples should be delivered to the customer for review and approval at least 30 days before acceptance tests.

Signal and Data Transmission System (DTS) Line Supervision

All signal and DTS lines should be supervised by the system. The system should supervise the signal lines by monitoring the circuit for changes or disturbances in the signal and for conditions described in *UL 1076: Standard for Proprietary Burglar Alarm Units and Systems* (1995) for line security equipment. The system should initiate an alarm in response to a current change of 10 percent or greater. The system should also initiate an alarm in response to opening, closing, shorting, or grounding of the signal and DTS lines.

Housing

Sensors and system electronics need different types of housing depending on their placement:

- **Interior sensors.** Sensors to be used in an interior environment should be housed in an enclosure that provides protection against dust, falling dirt, and dripping non-corrosive liquids.
- **Exterior sensors.** Sensors to be used in an exterior environment should be housed in an enclosure that provides protection against windblown dust, rain and splashing water, hose-directed water, and ice formation.
- **Interior system electronics.** System electronics to be used in an interior environment should be housed in enclosures that meet the requirements of *NEMA Standards Publication 250-2008: Enclosures for Electrical Equipment (1000 Volts Maximum)* (2008), Type 12.
- **Exterior system electronics.** System electronics to be used in an exterior environment should be housed in enclosures that meet the requirements of *NEMA Standards Publication 250-2008: Enclosures for Electrical Equipment (1000 Volts Maximum)* (2008), Type 4X.
- **Corrosive settings.** System electronics to be used in a corrosive environment as defined in NEMA 250 should be housed in metallic enclosures that meet the requirements of *NEMA Standards Publication 250-2008: Enclosures for Electrical Equipment (1000 Volts Maximum)* (2008), Type 4X.
- **Hazardous environments.** System electronics to be used in a hazardous environment should be housed in enclosures that meet the manufacturers' requirements for specific hazardous environments.

Nameplates

Laminated plastic nameplates should be provided for all major components of the system. Each nameplate should identify the device and its location within the system. Laminated plastic should be 1/8 in. (3.2 mm) thick and white with a black center core. Nameplates should be a minimum of 1 x 3 in. (25 mm x 76 mm), with minimum 1/4 in. (6.4 mm) high engraved block lettering. Nameplates should be attached to the inside of the enclosure housing the major component. All major components should also have the manufacturer's name, address, type or style, model or serial number, and catalog number on a corrosion-resistant plate secured to the equipment. Nameplates are not required for devices smaller than 1 x 3 inches (25 mm x 76 mm).

Tamper Switches

Enclosures, cabinets, housings, boxes, and fittings that have hinged doors or removable covers and that contain system circuits or connections and power supplies should be provided with cover-operated, corrosion-resistant tamper switches, arranged to initiate an alarm signal when the door or cover is moved. The enclosure and the tamper switch should function together and should not allow a direct line of sight to any internal components before the switch activates. Tamper switches should do the following:

- Be inaccessible until the switch is activated.
- Have mounting hardware concealed so the location of the switch cannot be observed from the exterior of the enclosure.
- Be connected to circuits that are under electrical supervision at all times, irrespective of the protection mode in which the circuit is operating.
- Be spring-loaded and held in the closed position by the door or cover.
- Be wired so they break the circuit when the door or cover is disturbed.

Locks

For maintenance purposes, locks should be provided on system enclosures. Locks should be a UL-listed, round-key type with three dual, one mushroom, or three plain-pin tumblers, or a conventional key lock with a five-cylinder pin and five-point, three-position side bar. Keys should be stamped "DO NOT DUPLICATE." The locks should be arranged so that keys can only be withdrawn in the locked position. Maintenance locks should be keyed alike, and only two keys should be furnished. The keys should be managed in accordance with a key control plan.

Wire and Cable

The contractor should provide all wire and cable not indicated as customer-furnished equipment. Wiring should meet NFPA 70 standards. The contractor should install the system in accordance with the standards for safety (NFPA 70, UL 681, UL 1037, and UL 1076) and the appropriate installation manual for each equipment type. Components within the system should be configured with appropriate service points to pinpoint system trouble in less than 20 minutes. The minimum conduit size should be ½ in (1.3 cm).

Local Area Network (LAN) Cabling

LAN cabling should be in accordance with the Telecommunications Industry Association/Electronic Industries Alliance standard EIA-568 A or B, category five.

Quality Assurance

All work should conform to the following codes:

- currently adopted National Electrical Code (NEC)
- applicable federal, state, and local codes
- currently adopted uniform building code
- local electrical code as applicable
- Occupational Safety and Health Act (OSHA) standards
- any additional codes effective at the job site
- Americans with Disabilities Act (ADA)

All materials should conform to the following codes:

- National Electrical Manufacturers Association (NEMA)
- American National Standards Institute (ANSI)
- Underwriters Laboratories, Inc. (UL)

12.9.4 TUNING THE SYSTEM

After installation, the system must be tuned to the operation of the facility. Otherwise, the system may generate too many unwanted alarms and confuse the operating personnel rather than assist them. Tuning the system requires knowing how the facility operates, what employees come and go, and what types of activities take place.

Time Periods for Alarms

To tune the system, the security manager should periodically run system reports and look at the alarm history, which shows nuisance alarms and alarm location, frequency, and timing. Patterns may emerge. For example, alarms may go off at certain times just because of day-to-day business. In those cases, the security manager can adjust the alarm operating times so that alarms will not be generated and security staff will not be unnecessarily distracted.

Responsibility for Monitoring Alarms

If an alarm associated with a loading dock door is constantly being received by the security monitoring center during business hours, then responsibility for monitoring of this alarm point should be transferred to personnel in that area. If alarms from mechanical or utility rooms are being received because maintenance personnel require access, procedures should be established to notify the central monitoring center that work will be performed in a

certain area for a specific time, allowing the security systems operator to temporarily ignore those particular alarm points. Secured doorways where material movement is controlled must have a procedure such as a phone call to the central station. A security guard may be needed to control access to those areas.

Authorized Personnel

If authorized personnel are trusted and allowed to enter areas any time, then alarms should be shunted so that an alarm will not be generated.

Nuisance Alarms

Many nuisance alarms are caused by employee mistakes, such as opening the wrong doors, holding doors open, or forgetting to disarm alarm subsystems. Other alarms may be caused by malfunctioning door hardware. Signage, such as “keep doors closed,” may help, as may adjusting guards’ patrol times so they are more likely to catch instances where employees go through doors and leave them open. Patrol officers should check all the doors and make sure they are closed. The security manager should also examine the maintenance program to ensure that doors are kept in good operation. Maintenance should include frequent door inspections and prompt replacement of faulty components.

Improper Application

Sometimes the security and fire alarm system components selected are wrong for their application. For example, standard motion detectors should not be placed in a harsh environment, and microwave sensors should not be used in a room that has a hallway outside. These devices should be changed to eliminate nuisance alarms.

12.9.5 MAINTAINING THE OPERATING PROCEDURES

It is important to periodically review the operating procedures. Whenever procedures are changed, they should be documented with a new revision number and date. Saving the old revisions makes it possible to ascertain what policies and procedures were in effect at certain times—useful information if the security manager ever has to defend past actions. It is also important to align rewards and consequences. In other words, the security manager should reward people who do go a good job in security and make clear that there are consequences if operating procedures are not followed.

Incident response policies should be reviewed periodically by legal counsel. The legal review should ensure that procedures

- are legally defensible and enforceable,
- comply with overall company policies and procedures,

- reflect known industry best practices demonstrating the exercise of due care,
- conform to national, state, and local laws and regulations, and
- protect staff from lawsuits.

In addition, legal counsel should consider the following factors:

- when to prosecute and what should be done to prosecute a person caught violating facility access rules
- what procedures will ensure the admissibility of evidence
- when to report an incident to local, state, or national law enforcement agencies

Legal counsel can help the security manager develop procedures and train security officers in such a way as to avoid problems that may lead to lawsuits over the following issues:

- **Failure to adhere to duty guidelines.** This occurs when officers engage in conduct beyond their established duties.
- **Breach of duty.** This occurs when officers engage in unreasonable conduct.
- **Proximate cause.** This term means an officer was the immediate cause of injury to a victim.
- **Foreseeability.** This term refers to events, especially those that could cause loss, harm, or damage, that the officers or management could have determined were likely to happen.

Failure to properly consider the human element and staff procedures when designing and installing new integrated security systems can turn a well-founded investment into an operational nightmare. Security managers can avoid this mistake by ensuring that their plans for security systems contain a complete analysis of how the systems will be operated and how the security force will respond to security incidents.

12.10 TRAINING

While terrorist threats and natural disasters are deemed newsworthy, the activities that protect facilities are often considered mundane. Nevertheless, all the technological and procedural precautions in the world will be ineffective if they are not executed properly. Through well-conceived, well-executed security training programs, personnel can be better prepared to prevent incidents from happening, respond properly to incidents that do arise, and contribute to recovery efforts more effectively. Without appropriate training, personnel are more likely to contribute to security risks accidentally.

12.10.1 **GENERAL TRAINING REQUIREMENTS**

The customer should require that the installation contractor or systems integrator submit a proposal to conduct training courses for designated personnel in the operation and maintenance of the PPS. The training should address all the systems being installed. For example, if a CCTV system is being installed along with other systems, the CCTV training should be concurrent with and part of the training for the other systems.

Training manuals and training aids should be provided for each trainee, and several additional copies should be provided for archiving at the project site. The training manuals should include an agenda, defined objectives for each lesson, and a detailed description of the subject matter for each lesson. The contractor should furnish audiovisual equipment and other training materials and supplies. When the contractor presents portions of the course by audiovisual material, copies of the audiovisual material should be delivered to the customer in the same media used during the training sessions. The contractor should also recommend the number of days of training and the number of hours for each day. Approval of the planned training content and schedule should be obtained from the customer at least 30 days before the training.

All personnel giving instruction should be certified by the equipment manufacturer for the applicable hardware and software. The trainers should have experience in conducting the training at other installations and should be approved by the customer.

12.10.2 **TRAINING TOPICS**

System Administration

This training focuses on determining and implementing system operational parameters and making any necessary operational adjustments. The first training class should be scheduled so that it is completed about 30 days before factory acceptance testing (if conducted) or site acceptance testing. By completing this training, system administrators will learn to use all system functions, including ID badge design and production, cardholder setup and access level assignment, access door programming, alarm setup and implementation, data storage and retrieval through reports, and system database backups. If CCTV systems are included in the PPS, the administrators will learn the architecture and configuration of the CCTV system, CCTV hardware specifications, and fault diagnostics and correction. A second training class should be conducted one week before the start of acceptance testing, and the system administrators should participate in the acceptance tests and reliability testing.

System Monitoring

This training focuses on day-to-day system operation. Upon completion of training, operators will know how to use system monitoring functions as determined by system administrative staff, including monitoring alarm events; monitoring personnel access to the facility; assessing, responding to, and clearing alarms and messages; monitoring access door status; and running routine reports. The first training class should be scheduled so that it is completed about 30 days before site acceptance testing begins. Upon completion of this course, each operator, using appropriate documentation, should be able to perform elementary operations with guidance and describe the general hardware architecture and system functionality.

This training should cover the following topics:

- general PPS hardware architecture
- functional operation of the system
- operator commands
- database entry
- report generation
- alarm assessment
- simple diagnostics

A second training class should be conducted about one week before the acceptance test, and the system operators should participate in the acceptance tests and reliability tests. The course should include instruction on the specific hardware configuration of the installed subsystems and should teach students how to operate the installed system. Upon completion of the course, each student should be able to start the system, operate it, recover the system after a failure, and describe the specific hardware architecture and operation of the system.

Alarm Assessment and Dispatch

This training teaches PPS operators to assess the cause of different alarm conditions and properly deal with them. Before this training is conducted, the customer and contractor should have developed the alarm assessment and response procedures discussed in Chapter 5. This training should be based on the alarm types that might be expected from the various PPS subsystems.

Incident Response

This training teaches the security response force about responding to different alarms and scenarios. Before this training is conducted, the customer and the contractor should have developed the incident response procedures discussed in Chapter 5. This training should be

based on the various scenarios that the response force might encounter when responding to an alarm condition.

System Troubleshooting and Maintenance

This training focuses on the internal workings of the PPS so that students can troubleshoot and repair most problems. Topics in this class include system networking communications and diagnostics; device configurations and programming; controller setup, wiring, and diagnostics; software troubleshooting; and device programming. The system maintenance course should be taught at the project site about two weeks prior to reliability testing, and these students should participate in the reliability tests. The training should cover the following:

- physical layout of each piece of hardware
- troubleshooting and diagnostic procedures
- repair instructions
- preventive maintenance procedures and schedules
- calibration procedures

IT Functions

This training is for personnel in the IT department who need to understand how the security system functions within a LAN/WAN network infrastructure. Topics in this class include network topologies and communications specific to each security subsystem, the impact of system functions such as digital video storage on network bandwidth, and the maintenance of data security.

System Overview

This training shows how the system will help meet overall security goals and objectives, how the system has been customized to meet operational requirements, and how to communicate security awareness to all employees.

12.11 TESTING AND WARRANTY ISSUES

The tests performed by the implementation team may involve equipment, personnel, procedures, or any combination of these. The ideal acceptance tests stress the system up to the established limits of site-specific threats. Tests should simulate actual threat conditions and provide conclusive evidence about the effectiveness of the security system.

Equipment performance testing is designed to determine whether equipment is functional, has adequate sensitivity, and will meet its design and performance objectives. It is not sufficient for a component to meet the manufacturer's standards if the component proves ineffective during testing. Equipment performance tests must always be coordinated with appropriate facility personnel.

Personnel performance tests are intended to determine whether procedures are effective, whether personnel know and follow procedures, and whether personnel and equipment interact effectively. Some personnel performance tests require that personnel be tested without their knowledge. Particular care must be exercised to ensure that these types of tests are well-coordinated and safety factors carefully considered.

This section describes four types of tests:

- pre-delivery or factory acceptance tests
- site acceptance tests
- reliability or availability tests
- after-acceptance tests

In determining what tests to conduct on security systems, several factors should be considered:

- prioritizing of site-specific threats
- identification of worst-case scenarios (lowest probability of detection, shortest amount of delay, various pathways into a facility)
- identification of system functions (detection, assessment, delay) that are most critical in protecting company assets
- determination of each subsystem's assumed detection probabilities and vulnerability to defeat
- determination of the time for assessment of incidents (immediate assessment versus delayed assessment)
- identification of the last possible points at which an adversary must be detected to allow adequate response by the facility protective force

- comparison of vulnerabilities against findings and resolution of past security inspections and incidents

Generally, original copies of all data produced during factory, site acceptance, and reliability testing should be turned over to the customer at the conclusion of each phase of testing, prior to approval of the test.

The customer should provide documentation to the equipment supplier or system integrator describing the testing that must be accomplished during the installation and commissioning of the system. This documentation describes the personnel, equipment, instrumentation, and supplies necessary to perform acceptance testing. This documentation also describes who will witness all performance verification and reliability testing. The contractor should be informed that written permission of the customer should be obtained before proceeding with the next phase of testing.

This section also discusses the related concept of warranty issues.

12.11.1 **FACTORY ACCEPTANCE TESTING**

Depending on the size and complexity of the system, the customer may require the contractor to assemble a test system including some or all of the system components, and then conduct tests to demonstrate that system performance complies with specified requirements in accordance with approved factory test procedures. The tests may be designed by the customer, or the customer may require the contractor to design the tests. The tests should be scheduled in advance of any installation of the new system, and the customer should attend and observe the tests. Model numbers of components tested should be identical to those to be delivered to the site. Original copies of all data produced during factory testing, including results of each test procedure, should then be delivered to the customer at the conclusion of factory testing for approval of the test. The test report should be arranged so that all commands, stimuli, and responses are correlated to allow logical interpretation.

The factory test setup should include the following:

- all security control center monitoring equipment
- at least one of each type of data transmission link, along with associated equipment, to provide a representation of an integrated system
- a number of local processors (field panels) equal to the number required by the site design
- at least one sensor of each type used

- enough sensor simulators to provide alarm signal inputs (generated manually or by software) to the system equal to the number of sensors required by the design
- at least one of each type of terminal device used
- at least one of each type of portal configuration with all facility interface devices as specified

Equipment for testing CCTV systems includes the following:

- at least four video cameras and each type of lens specified
- three video monitors
- video recorder (if required for the installed system)
- video switcher, including video input modules, video output modules, and control and applications software (if required for the system)
- alarm input panel (if required for the installed system)
- pan/tilt mount and pan/tilt controller if the installed system includes cameras on pan/tilt mounts
- any ancillary equipment associated with a camera circuit, such as equalizing amplifiers, video loss/presence detectors, terminators, ground loop correctors, surge protectors, or other in-line video devices
- cabling for all components

The customer should require a written report for the factory test indicating all the tests performed and the results. All deficiencies noted in the pre-delivery testing should be resolved to the satisfaction of the customer before installation and acceptance testing.

12.11.2 **SITE ACCEPTANCE TESTING**

The customer should require the contractor to develop a plan to calibrate and test all components, verify data transmission system operation, install the system, place the system in service, and test the system. Before conducting the site testing, the contractor should provide a report to the customer describing results of functional tests, diagnostics, and calibrations, including written certification that the installed, complete system has been calibrated and tested and is ready to begin site acceptance testing. This report should be received at least two weeks before the start of site testing. The report should also include a copy of the approved site acceptance test procedures.

Using the site acceptance test procedures, the contractor should demonstrate that the completed system complies with all the contract requirements. All physical and functional

requirements of the project should be demonstrated. Through performance testing, the contractor shows system reliability and operability at the specified throughput rates for each portal, as well as the Type I and Type II error rates specified for the completed system. The contractor should calculate nuisance and false alarm rates to ensure that the system yields rates within the specified maximums at the specified probability of detection for each subsystem.

The site acceptance test should be started after written approval has been received from the customer. The contractor should be instructed that the customer may terminate testing any time the system fails to perform as specified. Upon successful completion of the site acceptance test, the contractor should deliver test reports and other documentation to the customer before commencing further testing.

For the PPS acceptance tests, the following should be done:

- verification that the data and video transmission system and any signal or control cabling have been installed, tested, and approved as specified
- when the system includes remote control/monitoring stations or remote switch panels, verification that the remote devices are functional, communicate with the security monitoring center, and perform all functions as specified
- verification that the video switcher is fully functional and that the switcher software has been programmed as needed for the site configuration
- verification that all system software functions work correctly
- operation of all electrical and mechanical controls and verification that the controls perform the designed functions
- verification that all video sources and video outputs provide a full bandwidth signal
- verification that all input signals are terminated properly
- verification that all cameras are aimed and focused properly
- verification that cameras facing the rising or setting sun are aimed sufficiently below the horizon that they do not view the sun directly
- if vehicles are used near the assessment areas, verification of night assessment capabilities (including whether headlights cause blooming or picture degradation)
- verification that all cameras are synchronized and that the picture does not roll when cameras are switched
- verification that the alarm interface to the intrusion detection subsystem is functional and that automatic camera call-up is functional for all designated alarm points and cameras

- when pan/tilt mounts are used in the system, verification that the limit stops have been set correctly, that all controls for pan/tilt or zoom mechanisms are operative, and that the controls perform the desired function
- if pre-position controls are used, verification that all home positions have been set correctly and have been tested for auto home function and correct home position

The contractor should deliver a report describing results of functional tests, diagnostics, and calibrations, including written certification that the installed, complete system has been calibrated and tested and is ready for reliability testing. The report should also include a copy of the approved acceptance test procedures.

12.11.3 RELIABILITY OR AVAILABILITY TESTING

Reliability testing is best conducted in alternating phases of testing and evaluation to allow for validation of the tests and corrective actions. The reliability test should not be started until the customer notifies the contractor, in writing, that the acceptance testing has been satisfactorily completed, training (if specified) has been completed, and all outstanding deficiencies have been corrected. The contractor should provide one representative to be available 24 hours per day, including weekends and holidays (if necessary), during reliability testing. The customer should terminate testing whenever the system fails to perform as specified.

Phase I Testing

The reliability test should be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system should operate as specified. The contractor should make no repairs during this phase of testing unless authorized by the customer in writing. If the system experiences no failures during Phase I testing, the contractor may proceed directly to Phase II testing after receipt of written permission from the customer.

Phase I Assessment

After the Phase I testing, the contractor should identify all failures, determine causes of all failures, repair all failures, and deliver a written report to the customer. The report should explain in detail the nature of each failure, corrective action taken, and the results of tests performed; it should also recommend when to resume testing. About a week after receiving the report, the customer should convene a test review meeting at the job site to discuss the results and recommendations. At the meeting, the contractor should demonstrate that all failures have been corrected by performing appropriate portions of the acceptance tests. Based on the contractor's report and the test review meeting, the customer may set a restart date or may require that Phase I be repeated. If the retest is completed without any failures, the contractor may proceed directly to Phase II testing after receiving written permission

from the customer. Otherwise, the testing and assessment cycles continue until the testing is satisfactorily completed.

Phase II Testing

Phase II testing should be conducted 24 hours per day for 15 consecutive calendar days, including holidays, and the system should operate as specified. The contractor should make no repairs during this phase of testing unless authorized by the customer in writing.

Phase II Assessment

After the conclusion of Phase II testing, the contractor should identify all failures, determine causes of failures, repair failures, and deliver a written report to the customer. The report should explain in detail the nature of each failure, corrective action taken, and results of tests performed; it should also recommend when to resume testing. About a week after receiving the report, the customer should convene a test review meeting at the job site to discuss the results and recommendations. At the meeting, the contractor should demonstrate that all failures have been corrected by repeating any appropriate portions of the site acceptance test. Based on the contractor's report and the test review meeting, the customer may set a restart date or may require that Phase II testing be repeated. The contractor should not commence any required retesting before receiving written notification from the customer. After the conclusion of any retesting, the Phase II assessment should be repeated.

12.11.4 AFTER-IMPLEMENTATION TESTING

Several tests can be conducted after implementation, such as these:

- **Operational tests.** Operational tests are performed periodically to prove correct system operation but do not involve verification of equipment operating specifications, such as detection patterns of motion sensors or the exact distance a protected door is opened before alarming. Operational tests might check whether alarms activate correctly when protected doors are opened, whether motion sensors are activated when people walk in particular locations, or whether tamper switches or duress buttons work properly.
- **Performance tests.** Performance tests verify that equipment conforms with equipment or system specifications. These tests determine parameters such as probability of detection and may require measuring devices, calibrated instruments, or special testing methods.
- **Post-maintenance tests.** Post-maintenance tests are operational tests conducted after preventive or remedial maintenance has been performed on security systems to make sure the systems are working properly and according to specifications.

- **Subsystem tests.** Subsystem tests ensure that large parts of the system are all working together as originally designed. Coordinated portions might include detection with normal response and detection with delays.
- **Limited scope tests.** Limited scope tests are used to test a complex system, which is broken down into several subsystems or segments that are tested separately. This type of testing is useful when it is difficult and time-consuming to test the entire system at one time.
- **Evaluation tests.** Evaluation tests are periodic, independent tests of the PPS to validate the vulnerability analysis and ensure that overall effectiveness is being maintained. An evaluation test should be performed at least once a year.

12.11.5 **WARRANTY ISSUES**

The contractor should be required to repair, correct, or replace any defect for a period of 12 months from the date of issue of the certificate of practical completion. The common time for the contractor to report to the job site to address a warranty issue is within four hours of the problem report. Moreover, the contractor should hold a sufficient stock of spares to allow speedy repair or replacement of equipment. Waiting for manufacturers to replace or repair equipment is not acceptable.

The contractor should provide the customer with telephone and fax contact numbers for reporting all problems and defects. The warranty should include full maintenance of equipment in accordance with the manufacturer's recommendations. The contractor should record all service visits in a database and provide report forms to the customer. The report form should record the date and time the fault was reported, the nature of the reported fault, the date and time of the visit, the actual fault identified, and the remedial work carried out.

A few questions to consider about warranties are as follows:

- Will the PPS supplier provide the warranty service, or will a third party do so?
- Are the service levels of the warranty service consistent with the system maintenance service levels?
- If items under warranty fail, what will happen with respect to the maintenance services any other parties are providing?

12.12 MAINTENANCE, EVALUATION, AND REPLACEMENT

Organizations' increasing reliance on physical protection systems, coupled with the increasing scale and complexity of these systems, requires careful consideration of maintenance requirements. Software is never error-free, nor is hardware immune to electrical or mechanical failure. An organization's investment in security must therefore include maintenance services and a plan to minimize the potential for and impact of failures.

An effective maintenance program normally includes provisions that require facility technicians, augmented by contract representatives, to perform all tests, maintenance, calibrations, and repairs necessary to keep the physical protection systems operational. Frequent system failures, cursory testing procedures, and an inordinate number of components awaiting repair are all indications of a poor maintenance program. This section identifies the practical issues of hardware and software support and offers practical guidance for organizations considering a system maintenance agreement. Companies negotiating maintenance contracts should also seek legal advice as required. The section also raises the issue of evaluating whether and when to replace the physical protection system.

Physical protection system maintenance is of two main types:

- **Remedial maintenance.** This corrects faults and returns the system to operation in the event a hardware or software component fails. Remedial maintenance includes these measures:
 - establishing a maintenance function that acts on and logs requests from users in the event of a system problem
 - investigating the problem
 - resolving the problem directly or managing the resolution if third-party service is required
 - restoring the system or returning its use to the customer
 - updating documentation with respect to the problem and its resolution
- **Preventive maintenance.** This consists of scheduled maintenance to keep the hardware and software in good operating condition. Preventive maintenance includes these activities:
 - keeping electromechanical equipment (fans, filters, backup batteries, door hardware, etc.) operating correctly
 - replacing hardware components to keep the equipment up to current specifications (such as engineering changes)
 - updating system and application software (bug fixes, new versions, etc.)

- testing and analyzing system reports (error logs, self-tests, system parameters, performance measures, etc.)
- maintaining system documentation

Normally, a system maintenance agreement includes both categories of services.

A PPS requires all components to work together correctly to provide service to the users of the system. Failure of a single component may have no significant impact, or it may take the system down. A maintenance agreement should therefore be structured to resolve non-critical problems as well as issues that could cause major disruption to the organization and its business processes.

Common practice in the past has been for organizations to contract out the maintenance of their hardware, software, networks, and services separately. As systems have become more complex and integrated, the difficulties of identifying and resolving a problem or failure have increased. Not only is there the potential for finger-pointing between the parties over a problem, but the lost time of working through the various issues results in further frustration and delays.

Often the best solution is to select a single contractor to take responsibility for the maintenance requirements of the system. As the single point of contact, the contractor will diagnose the cause of the problem and manage the process of getting it resolved. Resolution may include third parties who supply or maintain particular system components, or it may require assistance from other service providers, such as telecommunication services or application software companies.

12.12.1 **REMEDIAL MAINTENANCE**

Maintenance Plan

Hardware and software system maintenance may be done by the equipment manufacturer, a system integrator, a maintenance contractor, the users, or any combination thereof. It is essential to develop guidelines to identify who is responsible for fault identification, problem diagnosis and verification, fault correction, repair testing, repair logging, and maintenance coordination and tracking. The coordination aspect is especially critical because security technologies may require several different types of maintenance skills depending on where a failure occurs.

It is also a good idea to train staff to perform preventive maintenance; this will help them better understand and operate the security systems. Such training is best provided by vendors as part of the procurement and installation phases of new systems. It is also useful to

give technicians time to upgrade their skills and knowledge by exchanging information with fellow technicians during the installation. In addition, the maintenance plan should consider periodic tuning of the security system to each facility to eliminate nuisance and false alarms that create problems for the personnel monitoring and responding to the system.

When contracting for maintenance services, the customer and the contractor should do the following:

- Agree on the basis of the contract document.
- Document in detail the components of the systems that are to be maintained.
- Set out the service levels for each component or subsystem.
- Define roles and responsibilities of the parties to the agreement.
- Agree on pricing and payments.
- Set out how the agreement will be managed and administered.

Service Levels

The failure of various components will have varying levels of impact on the system. Failure of a single camera will have a smaller impact than failure of the communications server for the entire network. However, another workstation on the network may support an essential security service and require high-priority service.

The customer and the contractor will jointly need to develop a support plan and the appropriate service level and response times for each component. Components whose failure has a high impact on the system require a higher level of support. The extreme case would require that an engineer be stationed on-site with full spares at hand. It is more likely that the customer will require a guarantee of an immediate return phone call from a maintenance technician and a response to a site within two to four hours. The customer should consider and specify service levels that are realistic, measurable, and in accord with the organization's specific business needs, particularly if travel is involved. The costs for guaranteed response times of less than four hours can escalate rapidly due to the staff hours, travel, and equipment required.

On the other hand, there may be components of the system that the customer elects not to include under the full maintenance plan. Personal computer workstations may already be covered by a maintenance agreement with the computer supplier. However, excluding some items from maintenance or having other items on lower levels requires careful thought.

Service levels and costs depend on the location of the system in relation to the supplier and on the ability to diagnose and fix problems remotely. Using a remedial maintenance provider

based in another city may significantly extend response times. Requiring support outside normal business hours also affects service levels and costs.

Roles and Responsibilities

The major goal of system maintenance agreements is to ensure that the security system operates at its optimum capability with minimum downtime. Another goal is to minimize the number of different parties involved in managing the maintenance program. Roles and responsibilities of all of the parties providing services must be clearly defined, documented, and agreed upon with the system maintenance supplier.

In some cases, the supplier of the maintenance service is also the supplier of the hardware and software or an agent of that supplier. However, usually the systems integrator takes responsibility for ongoing maintenance as the prime contractor.

In establishing a system maintenance agreement, it is necessary to develop a plan that denotes the responsibilities of all parties, establishes the company's central point of contact, and facilitates agreements between the parties. The following parties may be involved:

- hardware manufacturer or supplier
- systems integrator
- supplier of system tools and utilities where these are not provided by the hardware supplier
- supplier of the application software
- building owner (for such building services as power, water, and telephone/data circuits)
- air conditioning service provider (in relation to specific equipment in the security monitoring room)
- uninterruptible power supply (UPS) or emergency generator agent
- LAN and WAN equipment and service provider
- telecommunications service provider (for phones, leased data circuits, and private/public network access)
- PC supplier
- cabling supplier

The ideal may be for the prime vendor or systems integrator to manage all these parties in resolving faults or undertaking scheduled maintenance. Practically, that may not always be appropriate or cost-effective. Each customer may need to include or exclude specific third-party responsibilities.

Prices and Payments

Maintenance contractors usually have a scale of fees for the support of their products and for the delivery of their services. These fees may be arrived at from a complex mix of factors, including the complexity of the PPS, the cost of spare parts, the estimated number of failures per annum, the product usage frequency, the number of PPS users, and the age of the PPS. For high-volume or standard systems, the fee may simply be a set percentage of the purchase price. Support fees may also be affected by the geographic location of the system or the ability for online diagnosis and support. Alternatively, it may be agreed that travel and accommodation costs will be billed separately.

Economies of scale may also affect a supplier's pricing for maintenance support. A larger number of units or customers in a geographic location may provide the opportunity to pass on savings in travel, spare parts inventories, staff, training costs, and establishment costs.

Similarly, the payment cycle for maintenance costs may vary according to the scope and nature of the service required. One approach might consist of a fixed fee for an advance period (month, quarter, or year) plus an allowance or a formula for the following:

- discounts for the economies of longer-term contracts
- credits when target response times are not met
- additional costs associated with travel, accommodation, or work not covered by the agreement
- call-outs outside agreed business hours

Over time, the factors that dictate maintenance pricing change. Some may decrease, but the majority increase along with inflationary pressures or the aging of the products. It is usual for pricing review milestones to be built into a maintenance agreement and for there to be an understanding between the parties as to the size of any increases at these milestones. Not typically covered in a maintenance agreement are such items as misuse, vandalism, lack of training due to turnover, acts of God, etc.

Administration

System maintenance takes place in an environment that changes over the term of the contract. The agreement itself needs to be monitored and maintained to reflect such changes. The security manager should regularly review the agreement, measure the provider's performance, and address the agreement's scope. The review should cover the following issues:

- supplier performance against service levels and system performance for the previous period
- call logging and account management

- changes to the services or service levels that are required by the customer or recommended by the supplier
- changes to the list of equipment or software on the system
- customer's future plans for the system (including staffing, new developments, upgrades, special events, or changing priorities)

Documentation

The manufacturer or systems integrator should provide comprehensive documentation regarding the configuration of the system and all components, including switch settings, cable diagrams, spare parts lists, and installation steps. It is important that all subsystems have advanced levels of diagnostics that will identify faulty components so they can easily be replaced in the field. For a large, decentralized system, the ability to conduct remote diagnostics is especially helpful. Subscribing to an upgrade service for the hardware and software after installation guarantees that the latest engineering change orders and field change orders will be incorporated into the system, thereby extending the system's life.

Records

Keeping accurate records about the security systems—especially maintenance and operator records—can help the security manager in many ways. Knowing what parts are failing or causing operator problems can help identify trouble spots and deficiencies. Keeping track of costs helps justify replacing unreliable systems.

Maintenance Records

Maintenance records of all components, cross-referenced to subsystems, should be kept to identify repair patterns. These records may point to components that should be closely inspected during preventive maintenance. The maintenance contractor (or whoever does the system maintenance) should keep records and logs of each maintenance task and should organize cumulative records for each major component and for the complete system chronologically. A continuous log should be maintained for all devices. The log should contain calibration, repair, and programming data. Complete logs should be kept and made available for inspection on-site, demonstrating that planned and systematic adjustments and repairs have been accomplished for the security system.

System Operator Records

System operator records should be maintained to identify problems that operators have with certain subsystems or components. These reports should be analyzed periodically to identify problem subsystems and components and to update operating procedures.

Spare Parts

It is useful to procure spare parts and repair equipment in advance (perhaps as part of the original device procurement) to minimize downtime in the event remedial repairs are required. The appropriate quantity of spares on hand varies according to the time required to obtain spares, the cost of maintaining inventory, and the likelihood of replacement. As a rule of thumb, about 5 percent of the capital cost of equipment for a location should be allocated each year for spare parts purchases. Spare parts inventories should reflect vendor recommendations. Standardization of devices, through sole-source vendor relationships or tight procurement specifications, can reduce inventory needs as well as training needs. A centralized budget is recommended for paying for unexpected replacement of devices.

Maintenance Manuals

The contractor should provide the customer with a manual that describes maintenance for all equipment, including inspection, periodic preventive maintenance, fault diagnosis, and repair or replacement of defective components.

12.12.2 PREVENTIVE MAINTENANCE

Checklists should be developed to ensure that preventive maintenance tasks are performed adequately, and the checklists should incorporate any guidelines from equipment manufacturers. Preventive maintenance applies to most elements of the system infrastructure and includes such tasks as bulb replacement and camera lens cleaning.

Budgeting and resource allocation decisions must take into account not only security technicians but also information technology support. To conserve travel time, preventive maintenance activities should be pursued simultaneously with remedial maintenance activities to the extent possible. The following are typical tasks in preventive maintenance:

- Inspect the cabinets to ensure that voltage warning signs exist on equipment like power supplies.
- Ensure that security system warning signs, if installed, are in their proper location.
- Inspect enclosures for damage, unauthorized openings, and corrosion of metallic objects. Repair and paint as required.
- Inspect air passages and remove any blockage.
- Inspect, investigate, and solve conditions for unusual odors.
- Inspect locking devices. Repair as required.
- As equipment is operated and tested, listen to, investigate, and solve conditions for unusual noises.
- Inspect equipment mounting for proper installation.

- Inspect for loose wiring and components.
- Inspect electrical connections for discoloration or corrosion. Repair as required.
- Inspect electrical insulation for discoloration and degradation. Repair as required.
- Inspect equipment grounding components such as conductors and connections. Repair as required.
- Clean equipment. Remove debris, dirt, and other foreign deposits from all components and areas of non-encapsulated equipment, such as ventilated control panels.
- Tighten electrical connections.
- Torque all electrical connections to the proper design value.
- Perform operational tests periodically to prove correct subsystem operation, not necessarily to verify equipment operating specifications.
- Open protected doors.
- Walk into protected rooms.
- Test metal detectors by passing metal through the detection area.
- Prove operation of fence disturbance sensors by shaking the fence.
- Conduct visual checks and operational tests of the CCTV system, including switchers, peripheral equipment, interface panels, recording devices, monitors, video equipment electrical and mechanical controls, and picture quality from each camera.
- Check operation of duress buttons and tamper switches.

Adjustments

Periodic adjustments to security systems may have to be made to ensure that they are operating effectively. Detection patterns for motion sensors may have to be adjusted based on results of testing activities. Adjustments may need to be made to varifocal lenses on CCTV cameras to ensure that the proper scenes are being viewed.

Backup Equipment

Since security subsystems require power, an auxiliary power source consisting of batteries or generators must be available. Switchover must be immediate and automatic if the primary power source fails. In most cases, immediate and automatic switchover will not occur if a generator is the sole source of backup power; batteries are required, and the generator assumes the role once it obtains full power. To ensure effective operation of all devices, security managers should provide for a regular test and maintenance program. Such a program includes periodic testing of equipment and circuits including backup power, as well as thorough inspection of equipment and circuits by qualified service personnel. Records of these tests should include the test date, name of the person conducting the test, and results.

12.12.3 **EVALUATION AND REPLACEMENT**

At some point, the system will complete its useful life and the process of replacement will begin. To justify the replacement cost, the security manager should consider such factors such as the cost of maintenance, lack of spare parts, obsolescence of hardware and software, operating costs, and unreliability. Replacement may also be justified by new technologies and features that provide improved security, the ability to reduce manpower, or other benefits.

The security manager should form a team of stakeholders in the organization, including members of the company's IT group, to select a system that will meet all stakeholders' needs. Performance deficiencies in the old system, such as the inability to read multiple card technologies or poor system response time, need to be addressed. Possible future uses of the system and ID cards, such as a debit card function in the employee cafeteria, should also be incorporated.

The team should build in considerable expansion potential to accommodate future plans for additional sites, panels, and cards. The team should also begin gathering information from reputable companies supported by a nationwide network of integrators. It is also crucial to make sure the system's software will pass muster with the IT department, which would have to work with it, and with the human resources department, which will need a seamless interface between its employee database software and the security system software.

12.13 **SUMMARY**

This chapter described implementation of a PPS design. The use of systems integration and a structured process was emphasized. The relation between (1) goals and objectives, design, and analysis and (2) implementation was described. In addition, the details of implementing a PPS were described. These include the use of requirements, design specifications, drawings and cost estimates. The process of placing a contract and selecting a vendor for system implementation was reviewed at a high level. The chapter also included information on installation and operational details that must be considered, as well as training, testing, warranty issues, system maintenance, and replacement of the system.

APPENDIX A

ESTIMATION

Types of Cost Estimates

Several types of cost estimates are used in the implementation of physical protection systems: budgetary estimates, preliminary design estimates, and final design estimates.

Budgetary Estimates

Budgetary estimates are prepared during the initial planning phase for a new PPS. The goal is to arrive at a cost figure that can be used for getting the new PPS into the budget cycle. Depending on the company's procurement policies, the budget cycle may require that systems be identified and submitted for consideration several (as many as five) years before the planned implementation. Since these estimates are used for budgetary purposes, they have a large contingency, such as plus or minus 10 to 20 percent. These estimates are difficult to prepare without actually performing a good portion of the system design.

To prepare a budgetary estimate, the project manager can discuss costs with other companies that have recently installed systems and ask potential vendors to develop budgetary estimates. Another resource is the data developed by RSMeans, a company that provides construction cost information.

Preliminary Design Estimates

If the PPS project is part of a larger construction project, the process may require a preliminary design estimate. This estimate should be developed at the 50 percent design review stage and normally has a contingency of plus or minus 10 percent. Since the design of the system is well under way, draft specifications, drawings, and equipment schedules can be used to develop the costs. Potential vendors, too, can provide estimates.

Final Design Estimates

The estimate is refined as the project advances to 100 percent completion. At this point, the final design estimate is developed using the completed documents, drawings, and schedules. This estimate should have minimal contingency, on the order of plus or minus 5 percent.

Life-Cycle Cost

The actual cost of a PPS is its life-cycle cost. Life-cycle cost estimates include the following components:

- **Engineering and design costs.** These are the costs associated with the design of the PPS, such as determining the appropriate products to accomplish the functions specified and producing drawings showing equipment locations, subsystem connections, and details of wiring various devices.
- **Hardware.** The hardware costs include the original equipment plus startup spare parts.
- **Software.** The software costs are for the operating system and application system software necessary to operate the PPS.
- **Installation costs.** Installation costs include labor expended in installing equipment and software, labor to perform inspection, testing and commissioning, equipment rental, permits, bonding, supervision, and overhead.
- **Operating costs.** Operating costs include expenses for personnel, power consumption, and consumables (such as paper and ink cartridges).
- **Maintenance costs.** Maintenance costs include labor and spare parts for preventive and remedial maintenance.
- **Other costs.** Other costs include state and local taxes, profit (10 percent), performance bonding (3-5 percent) and contingency (5-10 percent).
- **Adjustments.** RSMeans data are based on national averages. For specific locations, the cost data may need to be adjusted.

Detailed Estimating Procedures

The following is a step-by-step process for preparing an estimate for a physical protection system:

- **Identify PPS subsystems.** Typical subsystems for a PPS include the following:
 - **Fences and barriers:** perimeter fences; enclosures or fences around critical utilities; and portable, fixed, and automatic barriers
 - **Security control center or monitoring subsystem:** consoles, workstations, computers, printers, recorders, and displays
 - **Access control subsystem:** card readers, badges, badge preparation equipment, door locking devices, door position sensing devices, turnstiles, drop gates, and mantraps
 - **CCTV subsystem:** cameras, switchers, recorders, mounts, enclosures, and monitors
 - **Intrusion detection interior and exterior subsystem:** intrusion detection sensors, alarm sounding devices, and display devices

- **Lighting:** lighting fixtures, mounts, enclosures, poles, and ballast
- **Power, control, and data distribution:** backup power, surge protection, raceways, grounding, conduit, wire, and cable
- **Communications subsystem:** communications network used to connect all subsystems, intercom, radio, network, and telephone equipment
- **Search equipment:** metal detectors, explosives detectors, and X-ray machines
- **Identify other installation activities.** Before PPS components can be installed, the site must be prepared as follows:
 - **Site civil or structural modifications:** grading, drainage, towers, foundations, fencing gates, and barriers
 - **Specialty construction:** guard houses, monitoring stations, and ballistic- and blast-resistant structures
- **Develop list of components for each subsystem.** This information can be obtained from equipment vendors' brochures and guidelines or from RSMeans publications.
- **Establish component prices.** Cost data can be obtained from vendors and from RSMeans.
- **Estimate installation labor.** System integrators and equipment manufacturers can provide information regarding how many personnel and how much time will be required to install each component. They can also report the normal hourly rates.
- **Identify required special equipment and rates.** For the specialty construction activities required to install a PPS, one must identify, for each activity, the number of personnel and hours required, any special equipment needed, and the rental cost of that equipment.
- **Use spreadsheet program.** Once all the information has been gathered, the project manager should construct a spreadsheet to compute the estimate for the project.

In summary, it is important to use actual cost data or recent quotes from vendors whenever possible. The RSMeans industry averages are useful, but they must be adjusted to specific locations. Also, because estimates contain some contingency, the project manager should expect variation when bids are received.

In addition, a quality review is essential. After gathering the data and preparing the estimate, the project manager should subject them to a comprehensive review process to ensure that all the components are listed and in the correct quantities. The review should also double-check the cost of labor and the number of personnel required for installing each component, make sure there have not been any recent price increases, and determine whether any ongoing or near-term changes at the site may affect the project.

Sample Estimate

Figure 12-11 shows a sample spreadsheet for an integrated PPS. The sample security system consists of the following components:

- 2 perimeter revolving doors
- 10 interior single-leaf doors
- 12 fixed CCTV cameras
- 1 pan, tilt, and zoom camera on the roof of the building
- 2 CCTV monitors
- 1 digital video recorder
- 1 computer monitor for access control

| Quantity | Description | Unit Cost | Extension | Labor |
|-----------|--------------------------------------------------|-------------|--------------------|--------------------|
| 1 | Revolving door | \$30,000.00 | \$30,000.00 | \$15,000.00 |
| 2 | 8 card reader control panel | \$1,000.00 | \$2,000.00 | \$1,000.00 |
| 1 | Access control software | \$1,000.00 | \$1,000.00 | \$500.00 |
| 11 | Proximity card reader | \$100.00 | \$1,100.00 | \$1,100.00 |
| 3 | 12 VDC batteries | \$20.00 | \$60.00 | |
| 10 | Request to Exit Motion Detectors | \$75.00 | \$750.00 | \$1,000.00 |
| 1 | 24 VDC power supply | \$87.00 | \$87.00 | \$100.00 |
| 10 | 24 VDC electric strikes | \$150.00 | \$1,500.00 | \$2,000.00 |
| 1 | Operator training | | | \$500.00 |
| 1 | PTZ CCTV camera, lens, and enclosure | \$2,500.00 | \$2,500.00 | \$2,500.00 |
| 12 | Fixed CCTV camera, varifocal lens, and enclosure | \$700.00 | \$8,400.00 | \$8,400.00 |
| Subtotals | | | \$47,397.00 | \$32,100.00 |

| Summary of Costs | | | | |
|-------------------------------------|--|--------------------|--------------------|--------------------|
| Components | | \$47,397.00 | | |
| Tax & Shipping (12%) | | \$5,687.64 | | |
| Installation Labor (\$100 per hour) | | | \$32,100.00 | |
| Subtotal | | | | \$85,184.64 |
| Profit (10%) | | | | \$8,518.46 |
| Subtotal | | | | \$93,703.10 |
| Performance Bond (4%) | | | | \$3,748.12 |
| Total Cost Estimate | | | | \$97,451.23 |

Figure 12-11
Sample Estimate

APPENDIX B

SPECIFICATION

A typical specification may be broken down into the following headings. Suggestions are provided for some specific items that may be overlooked. Most companies and local authorities produce impressive and voluminous contract conditions to protect themselves. The specification should adhere to three standard sections: general, products, and execution. The example that follows includes sample, additional subsections.

Model Specification

Part 1: General

Authority and Responsibility

In this section, state who is issuing the specification, who has responsibility for making any changes, and who should be contacted and in what manner for any questions and comments.

Summary

This section contains the following:

- overall project description: high-level description of the overall project if PPS is part of a larger construction project
- list of all documents included in the bid package
- PPS description: a high-level, general description of the system
- system operation: a brief description of how the system will be operated
- description of all products and services to be included in the contract, including the supply, installation, and connection of PPS components and cable

Objectives

This section lists the system objectives so all bidders can understand what the system is intended to achieve. The objectives should be SMART (specific, measurable, attainable, relevant, and time-bound).

Submittal Format

Here the customer describes the outline and format for the proposals and specifies all the items to be included in the submittal. This section should also specify all system options that should be priced separately. The evaluation process, evaluation criteria, and criteria weighting are also explained in this section. Clear instructions in this section will greatly simplify the proposal evaluation process.

Performance Specifications

When using the RFP method of procurement, the specification is given as functional performance requirements for the system and equipment. It is the responsibility of the bidders to select the most appropriate equipment to fulfill the objectives and requirements of the system. Certain items may be specified by manufacturer and model number when necessary to ensure compatibility or performance. Part of the proposal evaluation process is to assess the quality, reliability, and suitability of the equipment proposed.

Future Expansion

This section describes any capacity, capability, or performance expansion requirements.

System Interfaces

Here the customer indicates whether other systems will or might be connected or interfaced to this system.

Codes and Regulations

The installation should comply with all relevant regulations, such as the following:

- ADA: Americans with Disabilities Act
- ASCII: American Standard Code for Information Interchange
- ASTM: American Society for Testing and Materials
- EIA: Electronic Industries Alliance
- FCC: Federal Communications Commission
- NEC: National Electrical Code
- NEMA: National Electrical Manufacturers' Association
- NFPA: National Fire Protection Association
- UL: Underwriters Laboratories, Inc.

Customer-Supplied Materials and Services

This section lists any items provided by the customer, such as storage facilities, power supplies, or tools.

Scheduling

Here the customer states the likely time frame for contract placement and job completion.

Statement of Compliance

All bidders must include a statement that the system proposed and priced complies with the specification. Variations and suggestions for changing or improving the system should be listed and priced separately.

Indemnity and Insurance

The contractor should indemnify and keep indemnified the customer against injury to, or death of, any person and loss of, or damage to, any property arising out of or in consequence of the contractor's obligations under the contract and against all actions, claims, demands, proceedings, damages, costs, charges, and expenses in respect thereof. For all claims against which the contractor is required to insure, the insurance coverage should be a minimum of \$1 million or such greater sum as the contractor may choose in respect of any one incident. The contractor should be expected to produce evidence of sufficient insurance coverage to meet these requirements before any work is carried out on-site.

Bonds

A surety bond is a three-party instrument between a surety (or insurance company), the contractor, and the project owner or customer. The agreement binds the contractor to comply with the terms and conditions of a contract. If the contractor is unable to successfully perform the contract, the surety assumes the contractor's responsibilities and ensures that the project is completed. Below are the four types of contract bonds that may be required:

- **Bid.** This type of bond guarantees that the bidder on a contract will enter into the contract and furnish the required payment and performance bonds.
- **Payment.** This type of bond guarantees payment from the contractor to persons who furnish labor, materials, equipment, or supplies for use in the performance of the contract.
- **Performance.** This type of bond guarantees that the contractor will perform the contract in accordance with its terms.
- **Ancillary.** These are bonds that are incidental and essential to the performance of the contract.

Modifications and Variations

No modifications or variations to the contract should be permitted without the written consent of the customer.

Notification

The contractor should notify the customer immediately if any unforeseen circumstances are encountered during the course of the contract that may require modifications or variation. The contractor should then await instructions before proceeding with any part of the contract that may be affected.

Warranty

The contractor should be required to repair, correct, or replace any defect of any nature that may occur for a period of 12-24 months from the date of issue of the certificate of practical completion. The common time for the contractor to report to the job site to address a warranty issue is within four hours of the problem report. The problem should be corrected without undue delay.

Therefore, the contractor should hold sufficient stock of spares to allow speedy repair or replacement of equipment. Waiting for manufacturers to replace or repair equipment is not acceptable. The contractor should provide the employer with contact information for reporting all problems and defects. The warranty should include full maintenance of equipment in accordance with the manufacturer's recommendations. The contractor should have in operation a system whereby all service visits are recorded in a database, and a report form should be provided to the customer. The report form should record the date and time that the fault was reported, the nature of the reported fault, the date and time of the visit, the actual fault identified, and the remedial work carried out.

Maintenance

The contractor should submit a full schedule of maintenance to be carried out on the system during the warranty period and under subsequent maintenance contracts. This section should also state that the contractor must install all hardware and software updates and upgrades that become available during the time the system is being installed and is under warranty. This provision is included to protect the customer from having to accept a system that is obsolete upon installation.

Part 2: Products

This part of the specification lists equipment. One approach is to specify every item by manufacturer and model number. The advantage of that approach is that a totally objective comparison of all bids can be made. The disadvantage is that such specificity precludes the use of other, possibly less expensive or perhaps better makes of security devices that have performance characteristics as good as or better than those specified. By specifying one model, the customer provides an advantage to the company that has the best terms with that particular manufacturer. An alternative approach is to produce a performance-related specification with generic device descriptions. However, that approach requires especially careful bid assessment. Generally, a performance specification leads to the most competitive prices. Another commonly used technique is to specify a manufacturer and model number but follow it with the words "or equal."

The following are some of the product categories to list in this section:

- card readers
- access control panels
- ID cards
- workstations
- transmission of video and telemetry
- cameras
- lenses
- distribution amplifiers
- monitors
- camera housings
- pan, tilt, and zoom units
- video recorders
- multiplexers
- matrix switchers
- telemetry receivers
- quad units
- video printers
- consoles
- monitors
- cabling
- power supplies
- enclosures
- intercom equipment
- duress buttons
- motion detectors
- door contacts

Non-Proprietary Equipment

This section should state that all equipment, consoles, telemetry, switching and multiplexing devices, and other hardware must be commercially available, off-the-shelf products. This requirement ensures that future extensions to the system may be carried out by any installing company. The use of specialized, in-house manufactured components should not be allowed unless specifically requested as part of the requirements.

Part 3: Execution

Preparation of Site

Here the customer describes the condition of the site where the system will be installed and the work to be done by the contractor to prepare the site for the new system.

Installation and Quality Control Standards

This section states how inspections and quality control procedures will be conducted and records will be kept.

Trade Coordination

This section states whether coordination is required with other contractors regarding, for instance, fiber-optic cable installation or local-area network (LAN) or wide-area network (WAN) connectivity.

Subcontracting

No part of the contract should be subcontracted to any other company or individual without the express written permission of the customer. Unless specified to the contrary, it is assumed that all work will be carried out by the contractor. If the contractor intends to subcontract any part of the design or installation, that intention must be made clear in the bid submission and the name of the subcontractor should be provided. The customer should reserve the right to accept or reject nominated subcontractors.

Special Equipment

The contractor should normally be responsible for providing all special equipment necessary for safe installation of all high-level equipment. It should be the contractor's responsibility to provide all access equipment required to complete the installation in accordance with good safety practices.

Health and Safety

The contractor should be expected to comply with all health and safety requirements of the customer and of the authority having jurisdiction (AHJ).

Preassembly and Testing

All equipment should be prebuilt and tested at the contractor's premises before being delivered to the facility. The telemetry controls, multiplexer controls, and central recorder time/date generation should be assembled and proved to the satisfaction of the client's representative before being delivered to the site.

Testing and Commissioning

When the contract is considered to be complete, a certificate of completion should be issued after successful completion of reliability testing.

Operating Instructions

The contractor should provide a minimum of four full sets of operation manuals, operating instructions, descriptive brochures, and technical manuals for all subsystems included in the contract.

As-Built Drawings

The contract should require the contractor to provide as-built wiring and schematic diagrams.

Training

This section specifies what training will be required, over what period, and where. It also indicates what training manuals should be supplied and in what media. This section also states what qualifications (such as certifications from manufacturers) are required of the trainers.

Programming

Here the customer should ask the contractor to submit a list of all proposed programming activities, including device names, descriptions, timing, and sequence of operations. This section should also specify all programming to be done by the contractor for all subsystems.

Upgrades

The contractor should provide and install all hardware and software upgrades that become available for the PPS during the warranty period at no additional cost.

REFERENCES

- ASTM International. (2011). *Standard practice for security engineering symbols*. F967-03. West Conshohocken, PA: ASTM International.
- National Electrical Manufacturers Association. (2008). *NEMA standards publication 250-2008: Enclosures for electrical equipment (1000 volts maximum)*. Rosslyn, VA: National Electrical Manufacturers Association.
- National Fire Protection Association. (2011). *NFPA 70: National electrical code*. Quincy, MA: National Fire Protection Association.
- National Fire Protection Association. (2011). *NFPA 731: Standard for the installation of electronic premises security systems*. Quincy, MA: National Fire Protection Association.
- SIA/IAPSC. (1995). *Architectural graphics standard—CAD symbols for security system layout*. New York, NY: American National Standards Institute.
- TIA/EIA. (2001). *Commercial building telecommunications cabling standard*. TIA/EIA-568-B.1. Arlington, VA: Telecommunications Industry Association.
- Underwriters Laboratories. (1999). *UL 681: Standard for installation and classification of burglar and holdup alarm systems*. Camas, WA: Underwriters Laboratories.
- Underwriters Laboratories. (1999). *UL 1037: Standard for antitheft alarms and devices*. Camas, WA: Underwriters Laboratories.
- Underwriters Laboratories. (1995). *UL 1076: Standard for proprietary burglar alarm units and systems*. Camas, WA: Underwriters Laboratories.

INDEX

A

access control. *See* entry control, of personnel
acoustic concerns, 114, 127, 274
alarm communications, 91, 95, 129, 187
alarms, nuisance, 23, 34, 91, 93, 107, 159, 164, 303, 361, 369
analysis, 7, 20, 22, 25, 57, 129, 194, 301, 323
architecture, 41, 55, 61, 66, 79, 321, 326, 340, 345
assessment, 6, 10, 20, 23, 25, 61, 67, 93, 102, 107, 111, 135, 159, 166, 188, 302, 321, 364, 370
asset identification, 15
automated teller machines (ATMs), 75

B

balanced design. *See* balanced protection
balanced protection, 32, 106, 304
barriers, 39, 53, 68, 112, 248, 259, 297, 383
biometrics, 219, 223, 253

C

cameras, 70, 75, 77, 103, 112, 124, 134, 137, 142, 150, 154, 161, 170, 182, 215, 354, 369
clear zone, 108, 112, 159, 263
closed-circuit television (CCTV). *See* video
communications, security, 190
contingency planning, 32, 93, 113, 291, 315
contraband. *See* entry control, of contraband
crime prevention, 44, 60
crime prevention through environmental design (CPTED), 37

D

database, security, 13, 14, 140, 217, 254, 357, 389
defensible space, 42, 50, 78
delay, 23, 53, 112, 259, 303, 308
design basis threat, 10, 21, 92
design team, 56, 314, 333, 345
design, of physical protection system, 29, 31, 37, 93, 133, 141, 187, 248, 270, 297, 301, 320, 325
detection, 23, 34, 53, 90, 92, 217, 228, 260, 303, 326
dispensable barriers, 259, 273
documentation, 54, 129, 162, 308, 321, 335, 338, 378
doors, 63, 246, 267
drawings. *See* documentation
dual-technology sensors, 123

E

effectiveness, of security system, 9, 20, 23, 26, 31, 33, 161, 166, 188, 302, 306, 314, 366
electromagnetic energy, 127, 182, 192
entry control, of contraband, 217, 228, 252
entry control, of personnel, 23, 217, 218, 228, 239, 252, 329
environmental conditions, 37, 103, 107, 110, 127, 163
ergonomics, 211, 213
estimation, 382
evaluation, 21, 96, 112, 162, 166, 210, 301, 307, 372, 381, 386

F

federal buildings, 78, 223
fences, 21, 39, 48, 59, 82, 99, 108, 179, 263, 383
fire, 97, 245, 252, 276, 277, 281
floors, 32, 58, 119, 272, 284

G

gates, 47, 180, 252, 263
glass-break sensors, 117
goals and objectives. *See* problem definition
guards. *See* security officers

I

identification badges (IDs), 47, 219, 363
identification, of subjects in videos, 135, 144, 166, 227, 247
implementation, 5, 79, 319
information protection, 63
infrared sensors. *See* passive infrared (PIR) sensors
insider threat, 10, 114, 128, 255
installation, 95, 112, 129, 162, 251, 351, 383, 390
intrusion detection, 91, 93, 96, 97, 114
integration, 5, 23, 111, 130, 161, 251
intrusion detection, 128, 159, 216
invitation for bid (IFB), 347, 349

L

lamps, 71, 163, 169, 173, 175, 177, 178
laser communication, 204
lenses, 101, 123, 135, 138, 140, 145, 148, 151, 154, 171, 354
lighting, 39, 56, 60, 67, 70, 71, 75, 83, 103, 121, 125, 142, 163, 169, 215, 384
lightning, 93, 101, 111, 128, 274
line supervision, 130, 206, 352
locks, 38, 47, 228, 239, 268, 352, 359

loss impact, 6, 13, 15, 18, 19, 34, 301
luminaires, 70, 175, 179

M

magnetic locks, 247, 352
maintenance, 40, 71, 86, 113, 129, 163, 176, 253, 350, 365, 372, 373, 389
microbending, 118
microwave sensors, 102, 107, 112, 120, 361
microwave transmissions, 204
minimum consequence of component failure, 32
motion sensors, 116, 120, 371, 380

O

office buildings and office space, 61, 64, 161, 173, 324

P

parking facilities, 41, 64, 67, 72, 80, 179, 181, 183, 184, 264
parts, spare, 105, 129, 162, 377, 379, 383
passive infrared (PIR) sensors, 101, 106, 113, 121, 252, 353
performance measures, for PPS, 34, 218, 294, 303, 306
performance measures, for security staff, 35, 294
perimeter protection, 33, 58, 66, 71, 79, 99, 106, 109, 159, 179, 262, 263
personnel (as asset to protect), 1, 7, 10, 61, 274
personnel (as part of PPS), 1, 31, 34, 112, 130, 320, 325, 362, 365
probability of detection, 22, 32, 92, 99, 103, 107, 123, 371
problem definition, 1, 5, 26, 302, 365
procedures, 1, 22, 31, 34, 112, 128, 188, 253, 275, 284, 293, 361, 366
procurement, 176, 327, 329, 335, 347, 349
protection-in-depth, 31, 106, 130, 260, 304, 325

R

radiation, nuclear, 127, 233
radio frequency (RF) communications, 149, 194, 198, 293
radio frequency (RF) sensors, 126
replacement, of PPS equipment, 105, 162, 172, 177, 240, 361, 373, 379, 381
request for proposal (RFP), 348, 387
response, to alarms and incidents, 11, 23, 34, 53, 93, 106, 112, 160, 259, 262, 289, 291, 294, 313, 330, 361, 364, 375
risk assessment, 6, 9, 20, 25, 322, 325
risk management, 6, 8, 18, 321
roofs, 58, 65, 70, 272

S

safes, 64, 69, 276, 277, 279
schools, 72, 181, 252
scramblers, 200, 207
search technologies, 34, 229, 231, 235, 238, 252, 256, 384
security officers, 23, 36, 47, 57, 78, 112, 160, 259, 289, 294, 362
seismic issues, 99, 107, 110, 114, 128
sensors, exterior, 92, 97, 99, 105, 358
sensors, interior, 92, 104, 114, 116, 120, 127, 130, 358
signage, 41, 72, 74, 85, 247, 361
sole source, 347, 348
specification, 55, 92, 96, 154, 162, 170, 324, 329, 336, 386
standards, 75, 78, 83, 94, 134, 183, 265, 281, 282, 327, 337, 358, 360
surveillance, 34, 38, 49, 57, 70, 124, 151, 167, 182, 215
systems approach, 6

T

tampering, 91, 94, 109, 114, 121, 129, 206, 255, 359
target selection, 46
testing, of physical protection system, 22, 105, 109, 113, 129, 162, 166, 227, 304, 336, 363, 366, 370, 391
threat. *See* design basis threat
threat definition, 10, 22, 26, 235
training, 31, 34, 53, 112, 188, 290, 327, 362, 363, 391

U

Underwriters Laboratories (UL), 94, 276, 282, 357, 359

V

vaults, 64, 175, 281, 283
vehicle barriers, 261, 264, 297
vibration sensors, 116
video, 65, 70, 111, 124, 133, 169, 192, 289, 303, 354, 368, 389
video motion detectors, 103, 124
video recording, 75, 134, 138, 139, 142, 149, 156, 158, 164, 167, 303, 355
video transmission, 124, 138, 140, 149, 192, 203, 369
volumetric sensors, 98, 105, 116, 120, 121, 123
vulnerability assessment, 9, 10, 20, 67, 301, 302, 322

W

walls, 32, 58, 66, 69, 75, 119, 248, 266, 273, 284, 310
warranties, 163, 350, 372, 388
windows, 32, 38, 39, 47, 57, 63, 72, 75, 118, 270, 353
wireless sensors. *See* radio frequency (RF) sensors



1625 Prince Street
Alexandria, VA 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

ISBN 978-1-934904-37-4

